SAS/SATA II NAS System

User's Manual

Revision 1.0

P/N: PW0020000000386

Table of Contents

Preface 7

FCC Compliance Statement 8

Before You Begin 9

PART I Hardware Components and RAID Subsystem 10

Chapter 1 Introduction 11

1.1 Key Features 12
1.2 Technical Specifications 13
1.3 RAID Concepts 16
1.4 Array Definition 21
1.4.1 Raid Set 21
1.4.2 Volume Set 21
1.5 High Availability 22
1.5.4.1 Creating Hot Spares 22
1.5.4.2 Hot-Swap Disk Drive Support 22
1.5.4.3 Hot-Swap Disk Rebuild 22

Chapter 2 Installation Overview 23

2.1 Packaging, Shipment and Delivery 23
2.2 Unpacking the NAS System 23
2.3 Identifying Parts of the NAS System 24
2.3.1 Front View 24
2.3.2 Rear View 26

Chapter 3 Getting Started with the NAS System 28

3.1 Connecting the NAS to your Network 28
3.2 Powering On 28
3.3 Installing Hard Drives 30
3.4 Connecting SAS JBOD Enclosures and/or RAID with SAS JBOD 31

Chapter 4 RAID Configuration Utility Options 33

4.1 Configuration through Terminal 33
4.2 Configuration through the LCD Panel 39
4.2.1 Menu Diagram 40
4.3 Configuration through web browser-based proRAID Manager 45

Chapter 5 RAID Management 47

5.1 Quick Function 47
5.1.1 Quick Create 47
5.2 RAID Set Functions 49
5.2.1 Create RAID Set 49
5.2.2 Delete RAID Set 50
5.2.3 Expand RAID Set 51
5.2.4 Offline RAID Set 54
5.2.5 Activate Incomplete RAID Set 55
5.2.6 Create Hot Spare 57
5.2.7 Delete Hot Spare 57
5.2.8 Rescue Raid Set 58
5.3 Volume Set Function 59
5.3.1 Create Volume Set 59
5.3.2 Create Raid 30/50/60 62
5.3.3 Delete Volume Set 63
5.3.4 Modify Volume Set 64
5.3.4.1 Volume Set Expansion 65
5.3.4.2 Volume Set Migration 66
5.3.5 Check Volume Set 67
5.3.6 Schedule Volume Check 69
5.3.7 Stop Volume Check 70
5.4 Physical Drive 71
5.4.1 Create Pass-Through Disk 71
5.4.2 Modify a Pass-Through Disk 72
5.4.3 Delete Pass-Through Disk 72
5.4.4 Identify Enclosure 73
5.4.5 Identify Selected Drive 74
5.5 System Controls 75
5.5.1 System Configuration 75
5.5.2 EtherNet Configuration 77
5.5.3 Alert By Mail Configuration 78
5.5.4 SNMP Configuration 79
5.5.5 NTP Configuration 80
5.5.6 View Events / Mute Beeper 81
5.5.7 Generate Test Event 82
5.5.8 Clear Event Buffer 82
5.5.9 Modify Password 83
5.5.10 Upgrade Firmware 83
5.5.11 Restart Controller 83
5.6 Information Menu 84

5.6.1 RAID Set Hierarchy 84
5.6.2 System Information 85
5.6.3 Hardware Monitor 86

Chapter 6 System Maintenance 87

6.1 Upgrading the RAID Controller's Cache Memory 87
6.1.1 Installing Memory Module 87
6.2 Upgrading the RAID Controller's Firmware 88

PART II proNAS System 95

Chapter 7 Introduction 96

7.1 proNAS Key Components 96
7.2 Installation and Configuration Phases 97
7.3 Basic Setup Instructions in Creating Raid Set and Volume Set 98
7.4 Setting proNAS IP Address and Connecting to NAS Management GUI 101

Chapter 8 proNAS Manager 104

8.1 Volume Manager 105
8.1.1 Volume Group Management 106
8.1.1.1 Create the proNASVG Volume Group 106
8.1.1.2 Creating another Volume Group 109
8.1.1.3 Reset and Remove Volume Group 112
8.1.2 Logical Volume Configuration 114
8.1.2.1 Create new Logical Volume 114
8.1.2.2 Extending Logical Volume Size 116
8.1.3 Volume Snapshot 118
8.1.3.1 Create Snapshots Manually 119
8.1.3.2 Create Snapshots Based from Schedule 121
8.1.3.3 Delete Snapshots 124
8.1.4 Volume Replication 126
8.1.4.1 Replication Configuration 127
8.1.4.2 Checking the Status of Replication 132
8.1.4.3 Extending Logical Volume under Replication 133
8.1.5 iSCSI 134
8.1.5.1 iSCSI Configuration 134
8.1.5.2 Disable iSCSI in Logical Volume 137
8.1.5.3 Restore iSCSI to Ordinary Logical Volume 138
8.1.5.4 Extending iSCSI Logical Volume Size 140
8.2 Network Manager 142
8.2.1 Network Setting and Trunking 142
8.2.2 Internet Gateway 146

8.2.3 SNMP/MRTG 147
8.2.4 Network Test 148
8.3 Account Manager 149
8.3.1 External Accounts Integration (Joining Windows or NIS Domain) 149
8.3.1.1 Windows Authentication 149
8.3.1.2 Sample Steps to Join the NAS to Windows AD Domain: 150
8.3.1.3 NIS Authentication 152
8.3.1.4 Sample Steps to Join NIS Domain: 152
8.3.2 Local Account and Group Management 153
8.4 Share Manager 161
8.4.1 Share Management 162
8.4.1.1 Creating a New Share 162
8.4.1.2 Applying ACL 163
8.4.1.3 Modifying a Share 163
8.4.1.4 Deleting a Share 164
8.4.2 Properties Setting 165
8.4.2.1 Steps to Make a Share Folder a Public Folder Accessible to All Users: 166
8.4.3 Protocol Setting 167
8.4.3.1 CIFS 167
8.4.3.2 NFS 168
8.4.4 Privilege Setting (Permission) 169
8.4.4.1 Group 169
8.4.4.2 Account 170
8.4.4.3 IP Address 172
8.4.5 Rsync 174
8.4.6 Duplication 179
8.4.7 Default Share 183
8.5 System Manager 184
8.5.1 Information tab 185
8.5.2 Upgrade tab 186
8.5.3 Report tab 187
8.5.4 Time tab 188
8.5.5 Serial Ports tab 189
8.5.6 Power tab 190
8.5.7 Reboot tab 191
8.5.8 Service tab 192
8.5.9 Status tab 195
8.5.10 MRTG tab 196
8.6 Backup Manager 197
8.6.1 proNAS Configuration Backup 198

8.6.2 Configure Backup Plan....199
8.6.3 Tape Control....204
8.6.3.1 Backup and Restore Using Tape....205
8.7 Log Manager....221
8.8 Event Manager....222
8.8.1 E-mail Setting tab....222
8.8.2 Event Setting tab....223

Chapter 9 File Manager....225

9.1 Introduction to File Manager....225
9.2 Logon to File Manager....227
9.3 Directory and Upload Function....228
9.4 User Access Right and Group Access Right....230
9.5 Change Password and Logout....230

Chapter 10 proBackup....231

10.1 Introduction to proBackup....231
10.2 Administrator Logon....231
10.3 Create Backup Plan....234
10.4 Restore Backup....240
10.5 Account Detail....241

Chapter 11 proNAS HA (Optional Function)....242

11.1 Introduction to proNAS HA....242
11.2 Getting Started with proNAS HA....243
11.2.1 Hardware Aspect....244
11.2.2 Procedure for Setting Up proNAS HA....245
11.3 ProNAS HA Properties....254
11.4 Extending a Logical Volume in HA....255
11.5 Clear All HA Configuration....256
11.6 License Registration....258
11.7 Event Log Properties....259

Preface

About this manual

This manual provides information regarding the hardware features, installation and configuration of the **SAS/SATA II NAS System**. This document also describes the use of the storage management software. Information contained in the manual has been reviewed for accuracy, but not for product warranty because of the various environment/OS/settings. Information and specifications will be changed without further notice. Some pictures and screenshots might be different with the actual machine.

This manual uses section numbering for every topic being discussed for easy and convenient way of finding information in accordance with the user's needs. The following icons are being used for some details and information to be considered in going through with this manual:

NOTES:
These are notes that contain useful information and tips that the user must give attention to in going through with the subsystem operation.

IMPORTANT!
These are the important information that the user must remember.

WARNING!
These are the warnings that the user must follow to avoid unnecessary errors and bodily injury during hardware and software operation of the subsystem.

CAUTION:
These are the cautions that user must be aware of to prevent damage to the equipment and its components.

Copyright

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written consent.

Trademarks

All products and trade names used in this document are trademarks or registered trademarks of their respective owners.

Changes

The material in this document is for information only and is subject to change without notice.

FCC Compliance Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in residential installations. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

However, there is not guarantee that interference will not occur in a particular installation. If this equipment does cause interference to radio or television equipment reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna
2. Move the equipment away from the receiver
3. Plug the equipment into an outlet on a circuit different from that to which the receiver is powered.
4. Consult the dealer or an experienced radio/television technician for help

All external connections should be made using shielded cables

Before You Begin

Before going through with this manual, you should read and focus on the following safety guidelines. Information about the NAS system's packaging and delivery are also included. To provide reasonable protection against any harm on the part of the user and to obtain maximum performance, user is advised to be aware of the following safety guidelines particularly in handling hardware components:

Upon receiving of the product:

- Place the product in its proper location.
- To avoid unnecessary dropping out, make sure that somebody is around for immediate assistance.
- It should be handled with care to avoid dropping that may cause damage to the product. Always use the correct lifting procedures.

Upon installing of the product:

- Ambient temperature is very important for the installation site. It must not exceed 30°C. Due to seasonal climate changes; regulate the installation site temperature making it not to exceed the allowed ambient temperature.
- Before plugging-in any power cords, cables and connectors, make sure that the power switches are turned off. Disconnect first any power connection if the power supply module is being removed from the enclosure.
- Outlets must be accessible to the equipment.
- All external connections should be made using shielded cables and as much as possible should not be performed by bare hand. Using anti-static hand gloves is recommended.
- In installing each component, secure all the mounting screws and locks. Make sure that all screws are fully tightened. Follow correctly all the listed procedures in this manual for reliable performance.

Controller Configuration

This NAS system supports single RAID controller configuration.

Packaging, Shipment and Delivery

- Before removing the subsystem from the shipping carton, you should visually inspect the physical condition of the shipping carton.
- Unpack and verify that the contents of the shipping carton are complete and in good condition.
- Exterior damage to the shipping carton may indicate that the contents of the carton are damaged.
- If any damage is found, do not remove the components; contact the dealer where you purchased the subsystem for further instructions.

PART I Hardware Components and RAID Subsystem

Chapter 1 Introduction

The NAS System

Companies are looking for cost-effective storage solutions which can offer the best performance, high scalability and reliability. As the number of users and the amount of data grows, Network Attached Storage is becoming a critical technology and the need for an optimized solution is becoming an important requirement.

i-Stor delivers the " i-Stor iS16NS SAS NAS ", which combined direct attached storage (DAS), iSCSI target device and network attached storage (NAS) solution for flexible and expandable application, and together with the proNAS management solution, proNAS High-Availability and proBackup client backup solution, provide businesses with the most flexible, scalable, securable and manageable NAS environment. It helps to control the total cost of ownership for data management.

The i-Stor iS16NS is an SAS/SATA II NAS/DAS/iSCSI all in one Subsystem with proNAS 1.3 Operating System. It enhances system availability, and manages complex storage environments easily. For improving business productivity and minimizing business risks, i-Stor iS16NS provides a volume replication and a volume snapshot function. It is also a full featured data protection system supporting RAID levels 0, 1, 0+1, 3, 5, 6, 30, 50, 60 and JBOD. It supports hot spares, automatic hot rebuild and online capacity expansion within the enclosure.

1.1 Key Features

- Configurable to 19" rack-mountable 3U chassis
- INTEL Nehalem based
- Supports up to Sixteen (16) 1" hot - swappable SAS/SATA II hard drives
- Supports RAID levels 0, 1, 0+1, 3, 5, 6, 30, 50, 60 and JBOD
- Support NAS, DAS and iSCSI in one system
- Support two Gigabit Ethernet port for NAS file-sharing application
- Support one SAS port for direct access of RAID host connection
- Support iSCSI target for block level of IP storage environment
- Maximal support up to 224 SAS/SATAII disks totally based on:
  * Support one SAS Expansion port to connect up to 6 SAS JBOD enclosures for RAID expansion (up to 112 disks)
  * Support one SAS HBA port to connect second DAS enclosure to expand the RAID of NAS (up to next 112 disks with next 6 SAS JBOD)
- Smart-function LCD panel for RAID setting & ENC status
- Supports hot spare and automatic hot rebuild.
- Allows online capacity expansion within the enclosure
- Support spin down drives for power saving (MAID) and disk drive power cycle
- Schedule volume check data correctness by RAID 3/5/6
- 64 bit Linux-based embedded system
- Supports Tape/DAT backup/restore (Option)
- Centralization of Data and Storage Management
- Using Market-Leading Java Technology
- Latest volume snapshot technology
- Apply volume replication to enhance data protection
- Support logical volume over 2TB (Maximum 8 Exabytes)
- Data Backup via backup plan and scheduling
- Enhance system configuration backup
- Local and external account management, support large account import
- Share management and permission (support ACL setting)
- Support Internet Gateway function
- Online expansion file system
- Support E-mail notification and system log information
- Multi application support via proFamily

1.2 Technical Specifications

Hardware Platform
Intel Quad Core Xeon 2.0G or above, single / dual Processor
Cache memory : 3GB DDR3 SDRAM up to 32GB
Two Gigabit Ethernet ports (10 Gigabit Ethernet for additional option)
Up to Sixteen 1" hot-swappable SAS/SATA II (3Gb/s, NCQ support) hard drives
Real time drive activity and status indicators
Environmental monitoring unit
Two(2) 700W hot-swap power supplies with PFC
Expansion PCI slot for H/W upgrade
One (1) 4X SAS Host port for RAID connection to a Host System (volume created from enclosure is used by other host system)
One (1) 4X SAS Expansion port for JBOD connection (up to 6 SAS JBOD enclosures, max. 112 disks)
One(1) 4X SAS HBA port for connection to another DAS RAID and JBOD (max. 112 disks with 1 DAS + 6 JBOD enclosures)
RAID Controller Specifications
Intel IOP341 64 bit RISC
Supports RAID level: RAID 0, 1, 0+1, 3, 5, 6, 30, 50, 60 and JBOD
Supports 512MB up to 2GB of ECC cache memory
Supports hot spare and automatic hot rebuild
Support MAID (spin down drives when not in use to extend service)
Allows online capacity expansion within the enclosure
Built-in serial port interface for remote event notification
Local audible event notification alarm
Storage Management
Volume Management
Disk usage statistics
Hot spare capability

General
File Server Independent
Multiple language support
Support UPS management
System Management
Automatic IP address configuration
Self-contained unit - no extras needed
Management through Web browser
Flash upgradeable unit
SNMP / MRTG management and notification
Fail-free online firmware upgrade
Unicode support
Multi-node Management GUI
proNAS Data and Configuration Backup
Central Management
Networking
Supports NIC Trunking: Fault Tolerant, Load Balance, Fault Tolerant and Load Balance, and Link Aggregation 802.3ad
DHCP Server / DHCP Client
WINS Server
Internet gateway
Protocols
TCP/IP, SMB/CIFS, NFS, SNMP, FTP/SFTP/FXP, HTTP, Telnet, SSH
Supported Client Operating Systems
Microsoft® Windows® 98/ ME/ NT/ 2000 / XP / 2003 / Vista /2008
Unix / Linux
Mac OS

Authentication
Local User Account/Group
Microsoft NT Domain Controller (PDC)
Microsoft Active Directory Authentication (ADS)
Network Information Service (NIS)
Support batch creating users/Group
User quota management
Share level security
File level security
User ID security for NFS
Block Storage
iSCSI Target Support
Data Backup / Restore
Scheduling Multi-Snapshot
Replication
Duplication
Scheduling Rsync Replication
proBackup (backup from client to NAS)
Support CDP Server
High Availability
proNAS High Availability (optional)
Power requirements
AC 90V ~ 264V Full range
10A ~ 5A, 47~63Hz
Physical Dimension
133(H) x 482(W) x 716(D) mm

Note: Specifications are subject to change without notice. All company and product names are trademarks of their respective owners.

1.3 RAID Concepts

RAID Fundamentals

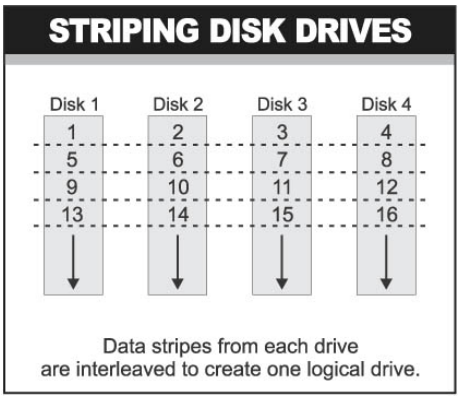
The basic idea of RAID (Redundant Array of Independent Disks) is to combine multiple inexpensive disk drives into an array of disk drives to obtain performance, capacity and reliability that exceeds that of a single large drive. The array of drives appears to the host computer as a single logical drive.

Five types of array architectures, RAID 1 through RAID 5, were originally defined; each provides disk fault-tolerance with different compromises in features and performance. In addition to these five redundant array architectures, it has become popular to refer to a non-redundant array of disk drives as a RAID 0 arrays.

Disk Striping

Fundamental to RAID technology is striping. This is a method of combining multiple drives into one logical storage unit. Striping partitions the storage space of each drive into stripes, which can be as small as one sector (512 bytes) or as large as several megabytes. These stripes are then interleaved in a rotating sequence, so that the combined space is composed alternately of stripes from each drive. The specific type of operating environment determines whether large or small stripes should be used.

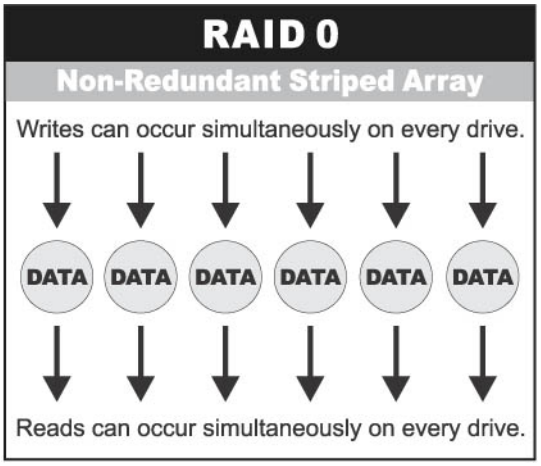
Most operating systems today support concurrent disk I/O operations across multiple drives. However, in order to maximize throughput for the disk subsystem, the I/O load must be balanced across all the drives so that each drive can be kept busy as much as possible. In a multiple drive system without striping, the disk I/O load is never perfectly balanced. Some drives will contain data files that are frequently accessed and some drives will rarely be accessed.



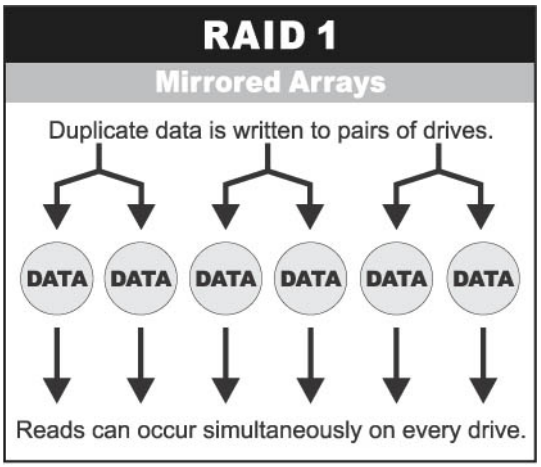
By striping the drives in the array with stripes large enough so that each record falls entirely within one stripe, most records can be evenly distributed across all drives. This keeps all drives in the array busy during heavy load situations. This situation allows all drives to work concurrently on different I/O operations, and thus maximize the number of simultaneous I/O operations that can be performed by the array.

Definition of RAID Levels

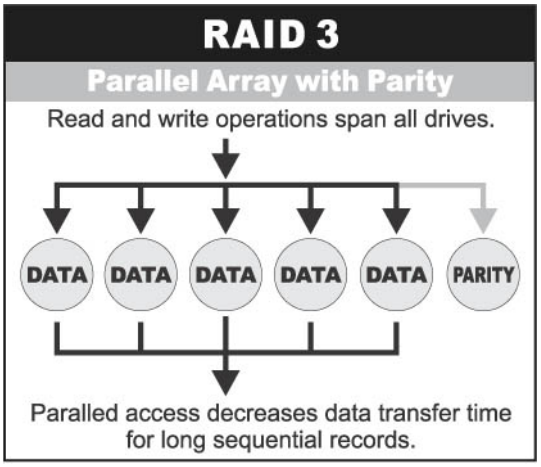
RAID 0 is typically defined as a group of striped disk drives without parity or data redundancy. RAID 0 arrays can be configured with large stripes for multi-user environments or small stripes for single-user systems that access long sequential records. RAID 0 arrays deliver the best data storage efficiency and performance of any array type. The disadvantage is that if one drive in a RAID 0 array fails, the entire array fails.



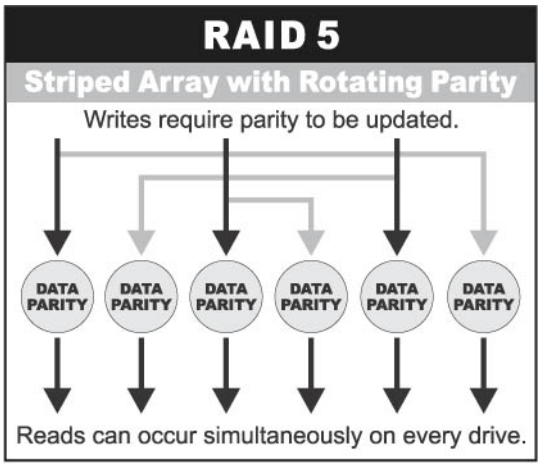
RAID 1, also known as disk mirroring, is simply a pair of disk drives that store duplicate data but appear to the computer as a single drive. Although striping is not used within a single mirrored drive pair, multiple RAID 1 arrays can be striped together to create a single large array consisting of pairs of mirrored drives. All writes must go to both drives of a mirrored pair so that the information on the drives is kept identical. However, each individual drive can perform simultaneous, independent read operations. Mirroring thus doubles the read performance of a single non-mirrored drive and while the write performance is unchanged. RAID 1 delivers the best performance of any redundant array type. In addition, there is less performance degradation during drive failure than in RAID 5 arrays.



RAID 3 sector-stripes data across groups of drives, but one drive in the group is dedicated for storing parity information. RAID 3 relies on the embedded ECC in each sector for error detection. In the case of drive failure, data recovery is accomplished by calculating the exclusive OR (XOR) of the information recorded on the remaining drives. Records typically span all drives, which optimizes the disk transfer rate. Because each I/O request accesses every drive in the array, RAID 3 arrays can satisfy only one I/O request at a time. RAID 3 delivers the best performance for single-user, single-tasking environments with long records. Synchronized-spindle drives are required for RAID 3 arrays in order to avoid performance degradation with short records. RAID 5 arrays with small stripes can yield similar performance to RAID 3 arrays.

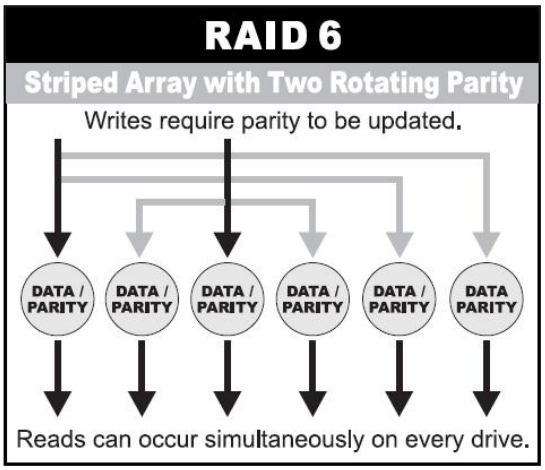


Under **RAID 5** parity information is distributed across all the drives. Since there is no dedicated parity drive, all drives contain data and read operations can be overlapped on every drive in the array. Write operations will typically access one data drive and one parity drive. However, because different records store their parity on different drives, write operations can usually be overlapped.



Dual-level RAID achieves a balance between the increased data availability inherent in RAID 1 and RAID 5 and the increased read performance inherent in disk striping (RAID 0). These arrays are sometimes referred to as RAID 0+1 or RAID 1+0 and RAID 0+5 or RAID 50.

RAID 6 is similar to RAID 5 in that data protection is achieved by writing parity information to the physical drives in the array. With RAID 6, however, ***two*** sets of parity data are used. These two sets are different, and each set occupies a capacity equivalent to that of one of the constituent drives. The main advantage of RAID 6 is High data availability – any two drives can fail without loss of critical data.



In summary:

- RAID 0 is the fastest and most efficient array type but offers no fault-tolerance. RAID 0 requires a minimum of one drive.
- RAID 1 is the best choice for performance-critical, fault-tolerant environments. RAID 1 is the only choice for fault-tolerance if no more than two drives are used.
- RAID 3 can be used to speed up data transfer and provide fault-tolerance in single-user environments that access long sequential records. However, RAID 3 does not allow overlapping of multiple I/O operations and requires synchronized-spindle drives to avoid performance degradation with short records. RAID 5 with a small stripe size offers similar performance.
- RAID 5 combines efficient, fault-tolerant data storage with good performance characteristics. However, write performance and performance during drive failure is slower than with RAID 1. Rebuild operations also require more time than with RAID 1 because parity information is also reconstructed. At least three drives are required for RAID 5 arrays.
- RAID 6 is essentially an extension of RAID level 5 which allows for additional fault tolerance by using a second independent distributed parity scheme (two-dimensional parity). Data is striped on a block level across a set of drives, just like in RAID 5, and a second set of parity is calculated and written across all the drives; RAID 6 provides for an extremely high data fault tolerance and can sustain multiple simultaneous drive failures. It is a perfect solution for mission critical applications.

RAID Management

The subsystem can implement several different levels of RAID technology. RAID levels supported by the subsystem are shown below.

RAID Level	Description	Min. Drives
0	Block striping is provide, which yields higher performance than with individual drives. There is no redundancy.	**1**
1	Drives are paired and mirrored. All data is 100% duplicated on an equivalent drive. Fully redundant.	**2**
3	Data is striped across several physical drives. Parity protection is used for data redundancy.	**3**
5	Data is striped across several physical drives. Parity protection is used for data redundancy.	**3**
6	Data is striped across several physical drives. Parity protection is used for data redundancy. Requires N+2 drives to implement because of two-dimensional parity scheme.	**4**
0+1 (1E)	Combination of RAID levels 0 and 1. This level provides striping and redundancy through mirroring. RAID 0+1 requires the use of an even number of disk drives to achieve data protection, while RAID 1E (Enhanced Mirroring) uses an odd number of drives.	**4 (3)**
30	Combination of RAID levels 0 and 3. This level is best implemented on two RAID 3 disk arrays with data striped across both disk arrays.	**6**
50	RAID 50 provides the features of both RAID 0 and RAID 5. RAID 50 includes both parity and disk striping across multiple drives. RAID 50 is best implemented on two RAID 5 disk arrays with data striped across both disk arrays.	**6**
60	RAID 60 combines both RAID 6 and RAID 0 features. Data is striped across disks as in RAID 0, and it uses double distributed parity as in RAID 6. RAID 60 provides data reliability, good overall performance and supports larger volume sizes. RAID 60 also provides very high reliability because data is still available even if multiple disk drives fail (two in each disk array).	**8**

1.4 Array Definition

1.4.1 Raid Set

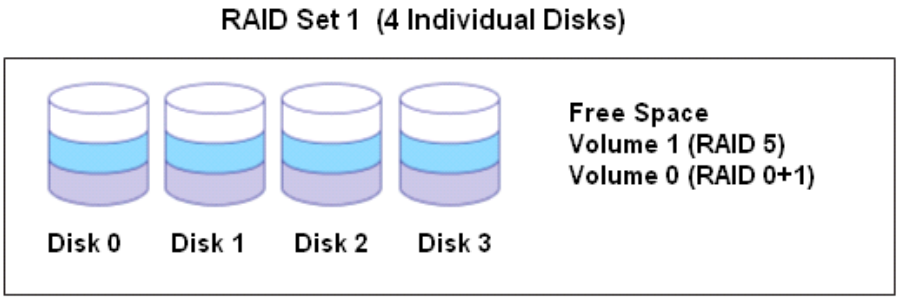
A Raid Set is a group of disk drives containing one or more logical volumes called Volume Sets. It is not possible to have multiple Raid Sets on the same disk drives.

A Volume Set must be created either on an existing Raid Set or on a group of available individual disk drives (disk drives that are not yet a part of a Raid Set). If there are existing Raid Sets with available raw capacity, new Volume Set can be created. New Volume Set can also be created on an existing Raid Set without free raw capacity by expanding the Raid Set using available disk drive(s) which is/are not yet Raid Set member. If disk drives of different capacity are grouped together in a Raid Set, then the capacity of the smallest disk will become the effective capacity of all the disks in the Raid Set.

1.4.2 Volume Set

A Volume Set is seen by the host system as a single logical device. It is organized in a RAID level with one or more physical disks. RAID level refers to the level of data performance and protection of a Volume Set. A Volume Set capacity can consume all or a portion of the raw capacity available in a Raid Set. Multiple Volume Sets can exist on a group of disks in a Raid Set. Additional Volume Sets created in a specified Raid Set will reside on all the physical disks in the Raid Set. Thus each Volume Set on the Raid Set will have its data spread evenly across all the disks in the Raid Set. Volume Sets of different RAID levels may coexist on the same Raid Set.

In the illustration below, Volume 1 can be assigned a RAID 5 level while Volume 0 might be assigned a RAID 0+1 level.



1.5 High Availability

1.5.4.1 Creating Hot Spares

A hot spare drive is an unused online available drive, which is ready to replace a failed disk drive. In a RAID level 1, 0+1, 3, 5 or 6 Raid Set, any unused online available drive installed but not belonging to a Raid Set can be defined as a hot spare drive. Hot spares permit you to replace failed drives without powering down the system. When the RAID subsystem detects a drive failure, the system will do automatic and transparent rebuild using the hot spare drives. The Raid Set will be reconfigured and rebuilt in the background while the RAID subsystem continues to handle system request. During the automatic rebuild process, system activity will continue as normal, however, the system performance and fault tolerance will be affected.

IMPORTANT: The hot spare must have at least the same or more capacity as the drive it replaces.

1.5.4.2 Hot-Swap Disk Drive Support

The RAID subsystem has built-in protection circuit to support the replacement of SATA II hard disk drives without having to shut down or reboot the system. The removable hard drive tray can deliver “hot swappable” fault-tolerant RAID solution at a price much less than the cost of conventional SCSI hard disk RAID subsystems. This feature is provided in the RAID subsystem for advance fault tolerant RAID protection and “online” drive replacement.

1.5.4.3 Hot-Swap Disk Rebuild

The Hot-Swap feature can be used to rebuild Raid Sets with data redundancy such as RAID level 1, 0+1, 3, 5 and 6. If a hot spare is not available, the failed disk drive must be replaced with a new disk drive so that the data on the failed drive can be rebuilt. If a hot spare is available, the rebuild starts automatically when a drive fails. The RAID subsystem automatically and transparently rebuilds failed drives in the background with user-definable rebuild rates. The RAID subsystem will automatically continue the rebuild process if the subsystem is shut down or powered off abnormally during a reconstruction process.

Chapter 2 Installation Overview

2.1 Packaging, Shipment and Delivery

- Before removing the subsystem from the shipping carton, you should visually inspect the physical condition of the shipping carton.
- Unpack the subsystem and verify that the contents of the shipping carton are all there and in good condition.
- Exterior damage to the shipping carton may indicate that the contents of the carton are damaged.
- If any damage is found, do not remove the components; contact the dealer where you purchased the subsystem for further instructions.

2.2 Unpacking the NAS System

The package contains the following items:

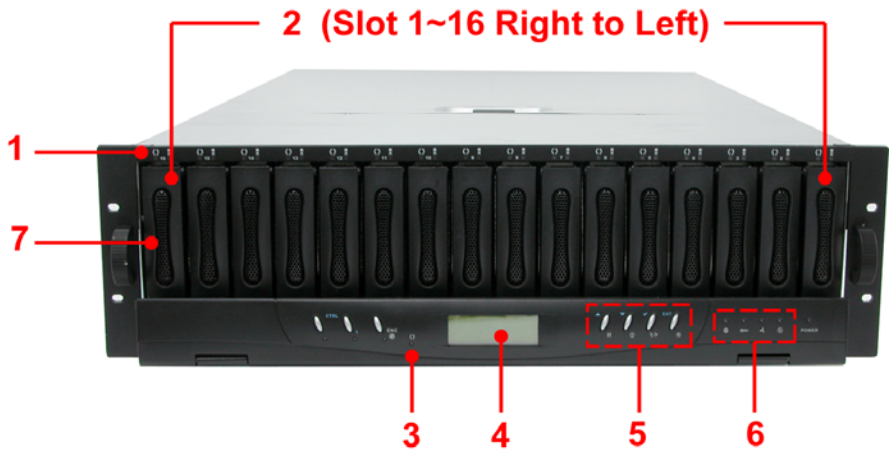
NAS System Unit	
Two (2) power cords	
Three (3) Ethernet LAN cables	
One (1) external serial cable	
One (1) USB-to-PS/2 converter cable	
Installation Reference Guide	
Spare screws, etc.	

If any of these items are missing or damaged, please contact your vendor or sales representative for assistance.

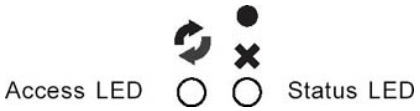
2.3 Identifying Parts of the NAS System

The illustrations below identify the various parts of the system. Familiarize yourself with the parts and terms as you may encounter them later in the later chapters and sections.

2.3.1 Front View



1. HDD Status Indicator



Parts	Function
HDD Status LED	Green LED indicates power is on and hard drive status is good for this slot. If there is no hard drive, the LED is Red. If hard drive defected in this slot or the hard drive is failure, the LED is blinking red.
HDD Access LED	This LED will blink blue when the hard drive is being accessed or busy.

2. HDD Trays 1 ~ 16 (From right to left)

3. Activity LED

The LED will be blinking blue when system is busy or data is being accessed.

4. LCD Display Panel

NOTE: The 3 buttons on the left of the LCD Display Panel are reserved (no function).

5. Smart Function Front Panel

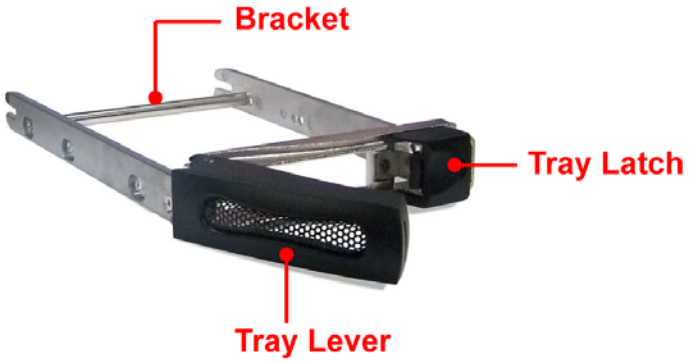
The smart LCD panel is an option to configure the RAID subsystem. If you are configuring the subsystem using the LCD panel, press the Select button to login and configure the RAID subsystem.

Parts	Function
Up and Down Arrow buttons	Use the Up or Down arrow keys to go through the information on the LCD screen. This is also used to move between each menu when you configure the subsystem.
Select button	This is used to enter the option you have selected.
Exit button **EXIT**	Press this button to return to the previous menu. NOTE: This button can also be used to reset the alarm beeper. For example, if one power supply fails, pressing this button will mute the beeper.

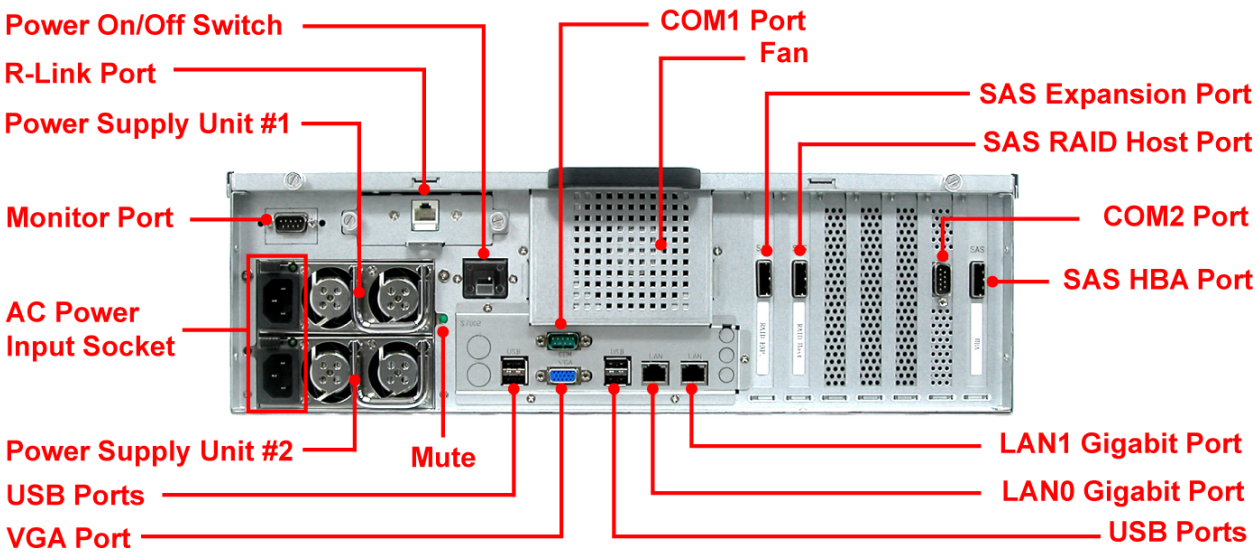
6. Environment Status LEDs

Parts	Function
Power LED	Green LED indicates power is ON.
Power Fail LED	If a redundant power supply unit fails, this LED will turn to RED and alarm will sound.
Fan Fail LED	When a fan fails or the fan's rotational speed is below 1500RPM, this LED will turn red and an alarm will sound.
Over Temperature LED	If temperature irregularities in the system occurs (HDD slot temperature over 65°C), this LED will turn RED and alarm will sound.
Voltage Warning LED	An alarm will sound warning of a voltage abnormality and this LED will turn red.

7. Disk Tray



2.3.2 Rear View



1. **Power On/Off Switch** – Use this switch to power on the NAS system. Note that there is a protective cover.

2. **R-Link Port** – The system is equipped with one 10/100 Ethernet RJ45 LAN port for remote RAID configuration and monitoring. Use a web browser to manage the RAID controller through proRAID Manager GUI.

3. **Monitor Port** – The system is equipped with a serial monitor port allowing you to connect a PC or terminal and manage the RAID controller.

4. **AC Power Input Socket** - Use this to connect the power cords connected from power source.

5. **Power Supply Unit #1 and #2** – Two power supplies (PSU 1 and PSU 2) are located at the rear of the NAS system.

   If the power supply fails to function, the Power Fail LED will turn red and an alarm will sound. An error message will also appear on the LCD screen warning of power failure.

6. **USB Ports** – The NAS system has four USB 2.0 ports.

NOTE: When connecting PS/2 keyboard and mouse, use the USB-to-PS/2 converter cable, and then insert the USB connector of converter cable to the one of the USB ports of the NAS.

7. **Fan**

8. **LAN0 and LAN1 Gigabit ports –** The NAS system has two Gigabit data ports. LAN0 is also used for configuring the NAS system via proNAS Manager.

9. **VGA Port** – Use this to connect a VGA monitor.

10. **COM1 and COM2 Serial Ports** – The NAS system has 2 serial ports.

11. **SAS Expansion Port** – Use this to connect SAS JBOD expansion enclosures to expand the storage capacity of the NAS. Up to 6 JBOD enclosures can be connected in daisy-chain.

12. **SAS RAID Host Port** – Use this to connect the RAID subsystem to a Host system's SAS HBA. The host system will detect the RAID volume created from the NAS RAID controller.

13. **SAS HBA Port** – Use this to connect another SAS RAID subsystem to expand the storage capacity of the NAS. The SAS RAID subsystem can include 6 JBOD enclosures connected in daisy-chain. The NAS will detect all volumes created from the SAS RAID subsystem.

Chapter 3 Getting Started with the NAS System

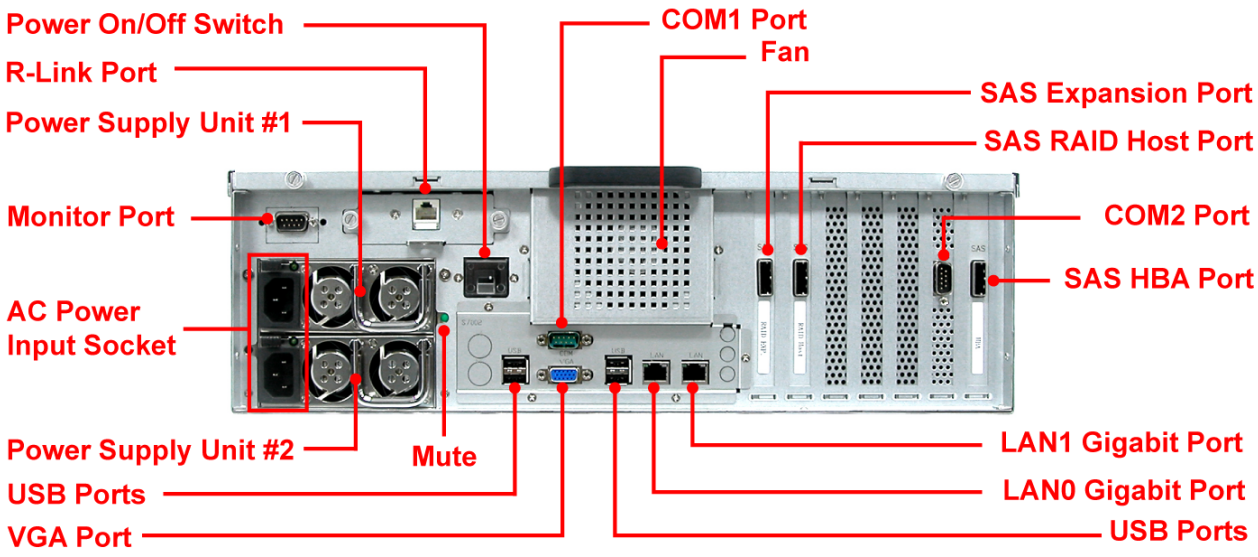
3.1 Connecting the NAS to your Network

1. For purpose of RAID configuration, attach network cable to the R-Link port. Connect the other end to your network hub or switch. Alternatively, you may use the Monitor port and connect the serial cable from the Monitor port to any available COM port of a PC.
2. Attach network cable to the Ethernet port LAN0. Connect the other end to your network hub or switch. You may also connect the other Ethernet port if needed.

3.2 Powering On

NOTE: If other JBOD subsystem(s) or RAID subsystem, with or without JBOD subsystem(s) connected in daisy-chain, are to be connected to the SAS Expansion Port or to the SAS HBA Port respectively, the JBOD subsystems or RAID subsystem (and its JBOD subsystem(s) must be powered on first before the NAS. This is to detect the disk drives from the JBOD subsystem or the volumes from the RAID subsystem. Refer to Section 3.4 for more information.

1. Plug in the 2 power cords into the AC Power Input Socket located at the rear of the NAS system.



NOTE: The NAS system is equipped with redundant, full range power supplies with PFC (power factor correction). The system will automatically select voltage.

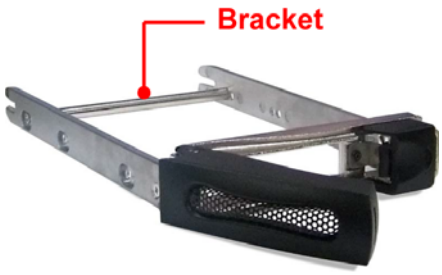
2. Open the protective cover of the Power On/Off Switch.
3. Turn on the Power On/Off Switch to power on the NAS.
4. The Power LED on the front Panel will turn green.

3.3 Installing Hard Drives

This section describes the physical locations of the hard drives supported by the subsystem and give instructions on installing a hard drive. The subsystem supports hot-swapping allowing you to install or replace a hard drive while the subsystem is running.

a. Pull out an empty disk tray. Press the tray latch downwards to release the tray. Pull the handle outwards to remove the carrier from the enclosure.

b. Take off the bracket before installing hard drive.



c. Place the hard drive in the disk tray.

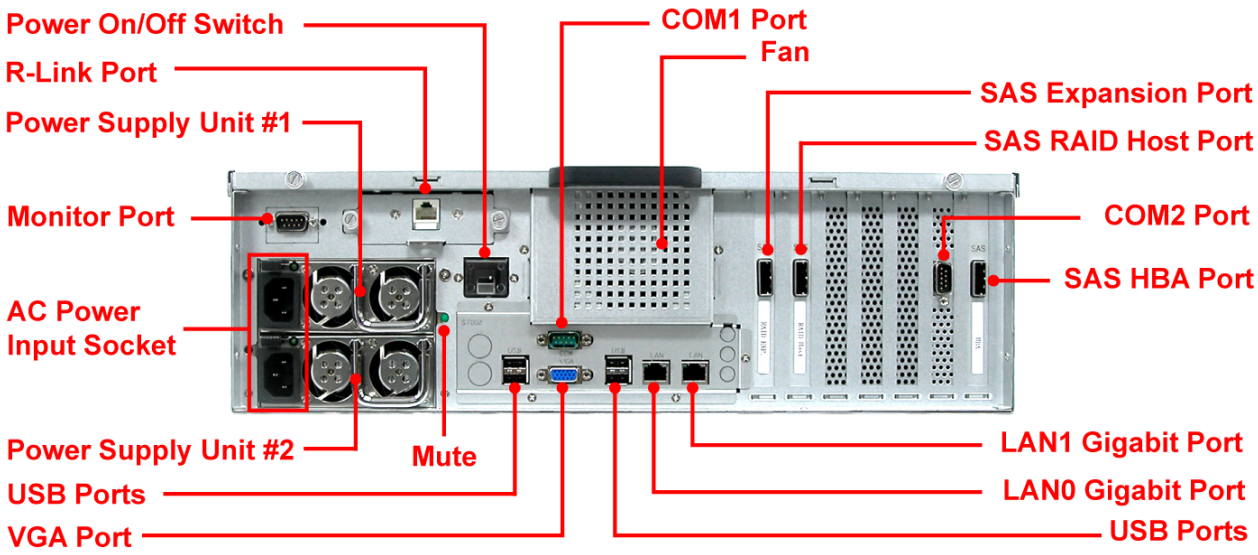
d. Install the mounting screws on each side to secure the drive in the tray.

e. Slide the tray into a slot and close the tray lever until it clicks into place. The HDD status LED will turn green if system is on.

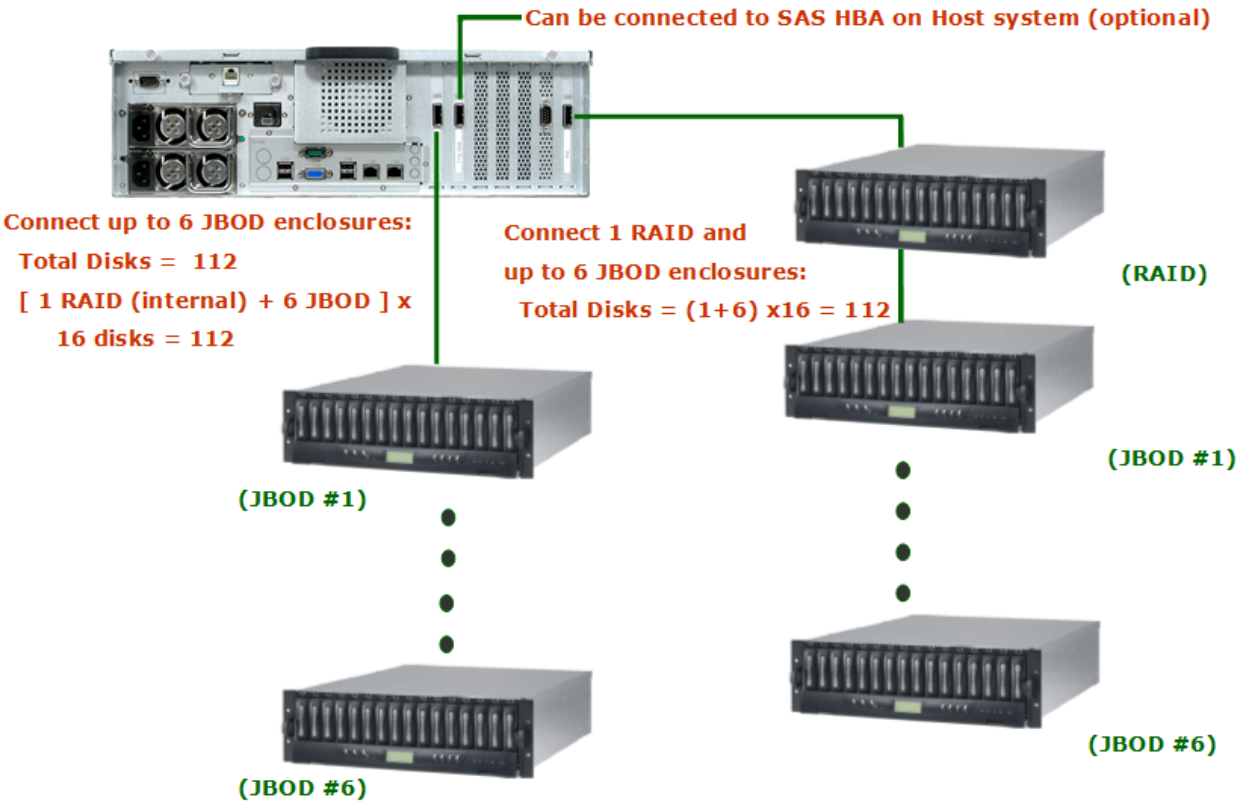
f. If the HDD power LED did not turn green, check if the hard drive is in good condition. If the hard drive is not being accessed, the HDD access LED will not illuminate.

3.4 Connecting SAS JBOD Enclosures and/or RAID with SAS JBOD

1. To connect JBOD enclosure, use mini SAS cable. Insert one end to the SAS Expansion Port of the NAS, and insert the other end to the SAS In port of the JBOD enclosure (JBOD#1).



2. If there are other JBOD enclosures to be connected, connect the SAS cable from the SAS Expansion Port of JBOD #1 to the SAS In Port of the next JBOD enclosure (JBOD #2). Repeat the process until the last JBOD is connected in daisy-chain.
3. If a RAID subsystem will be used, connect the SAS cable from the RAID subsystem's SAS Host Channel A (or Host Channel B, if needed) to the SAS HBA Port of the NAS.
4. If a JBOD enclosure will be connected to the RAID subsystem in daisy-chain, connect the RAID subsystem's SAS expansion port to the JBOD enclosure's SAS In Port (JBOD#1). If there are other JBOD enclosures to be connected, connect the SAS cable from the SAS Expansion Port of JBOD #1 to the SAS In Port of the next JBOD enclosure (JBOD #2). Repeat the process until the last JBOD is connected.


Can be connected to SAS HBA on Host system (optional)
Connect up to 6 JBOD enclosures:
Total Disks = 112
[1 RAID (internal) + 6 JBOD] x
16 disks = 112
Connect 1 RAID and
up to 6 JBOD enclosures:
Total Disks = (1+6) x16 = 112
(RAID)
(JBOD #1)
(JBOD #1)
(JBOD #6)
(JBOD #6)

5. Connect power cords to the AC Power Input Sockets of the JBOD enclosures and RAID enclosure, as applicable.
6. Power on the JBOD enclosures starting from the last enclosure in the chain. And power on the RAID enclosure.
7. Power on the NAS.
8. Insert the disk trays with disk drives.
9. Open proRAID Manager GUI (connect via R-Link port of NAS).
10. Check if the disk drives of the JBOD enclosures are detected in proRAID Manager.

Chapter 4 RAID Configuration Utility Options

Configuration Methods

There are four methods of configuring the RAID controller:

a. VT100 terminal connected through the serial Monitor port

b. Front panel touch-control buttons

c. Web browser-based remote RAID management via the R-Link Ethernet port

d. Telnet connection via the R-Link Ethernet port

NOTE: The RAID subsystem allows you to access using only one method at a time. You cannot use more than one method at the same time.

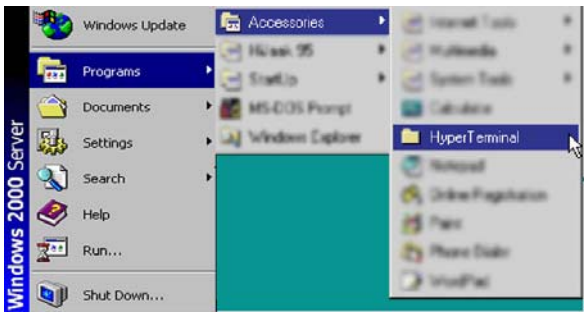
4.1 Configuration through Terminal

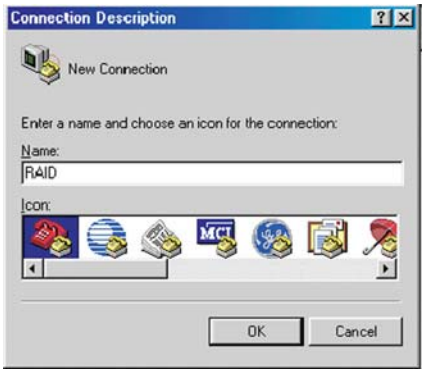
Configuring through a terminal will allow you to use the same configuration options and functions that are available from the LCD panel and via Telnet. To start-up:

1. Connect the Monitor port located at the rear of the system to another PC or a VT100 compatible terminal operating in an equivalent terminal emulation mode using serial cable.

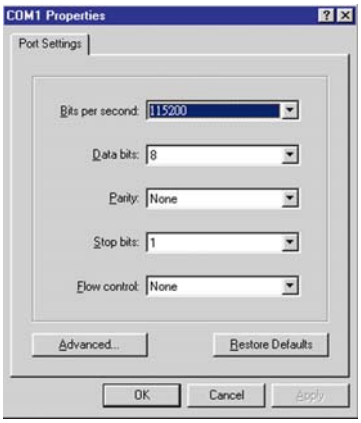
NOTE: You may connect a terminal while the system's power is on.

2. Power-on the terminal.
3. Run the VT100 program or an equivalent terminal program.

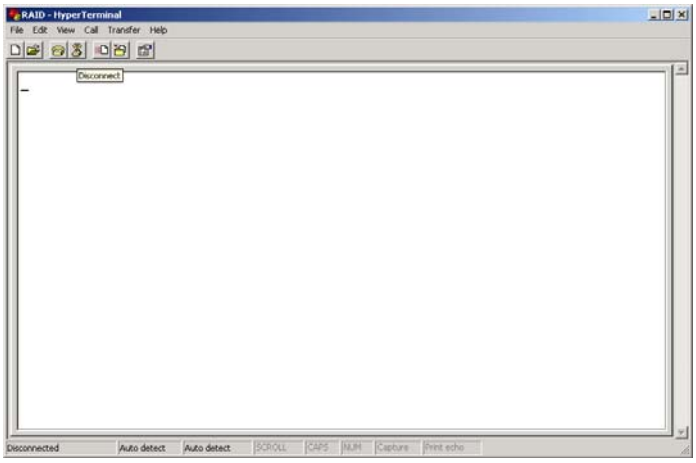




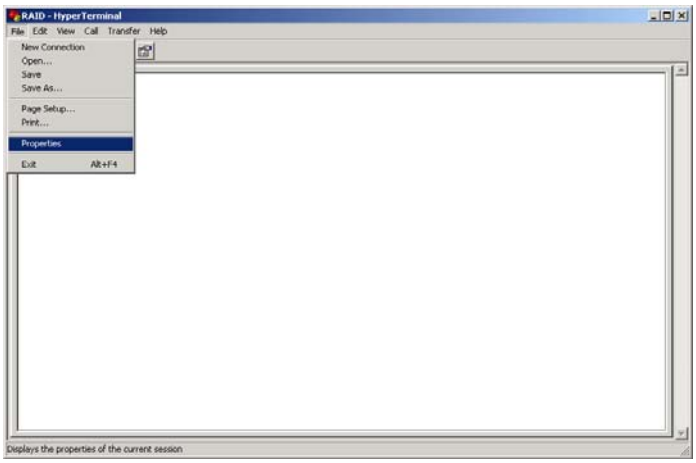
4. The default setting of the monitor port is 115200 baud rate, 8 data bit, non-parity, 1 stop bit and no flow control.



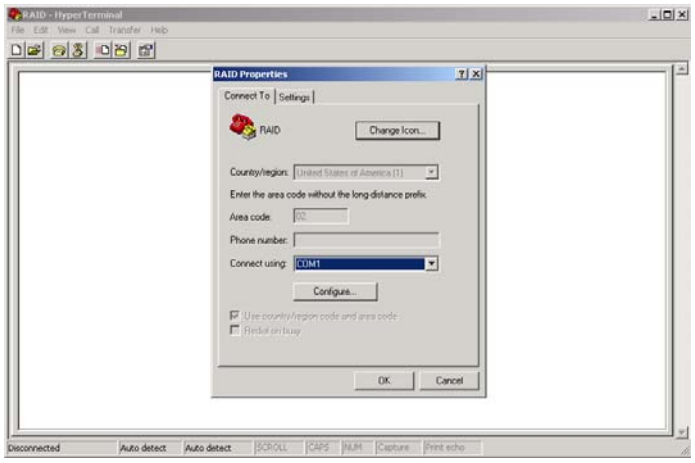
5. Click disconnect button.



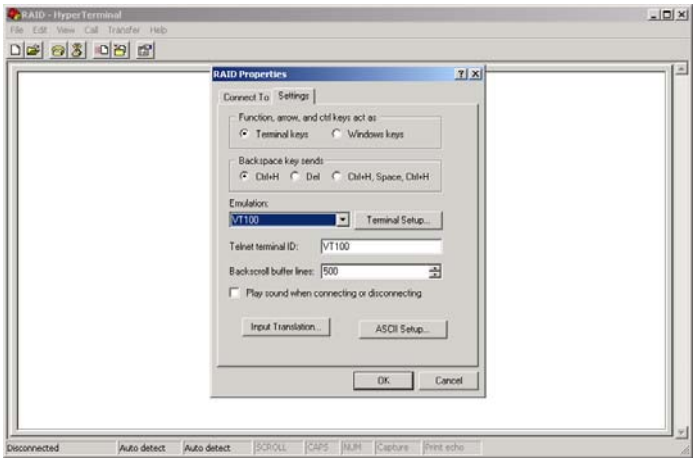
6. Open the File menu, and then open Properties.



7. Open the Settings Tab.

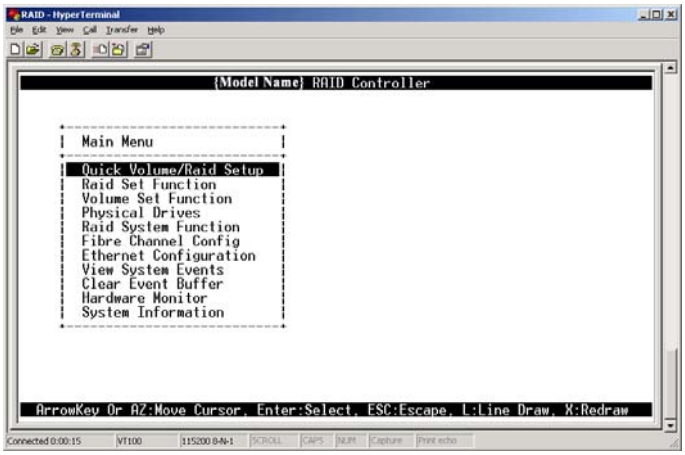


8. Configure the settings as follows:
   "Function, arrow and ctrl keys act as": Terminal Keys
   "Backspace key sends": Crtl + H
   "Emulation": VT100
   "Telnet terminal ID": VT100
   "Back scroll buffer lines": 500
   Click OK.



9. Now, the VT100 is ready to use. After you have finished the VT100 Terminal setup, you may press the “X” key (in your Terminal) to link the RAID subsystem and Terminal together. Press “X” key to display the disk array Monitor Utility screen on your VT100 Terminal.

10. The Main Menu will appear.



Keyboard Function Key Definitions

“A” key - to move to the line above

“Z” key - to move to the next line

“Enter” key - Submit selection function

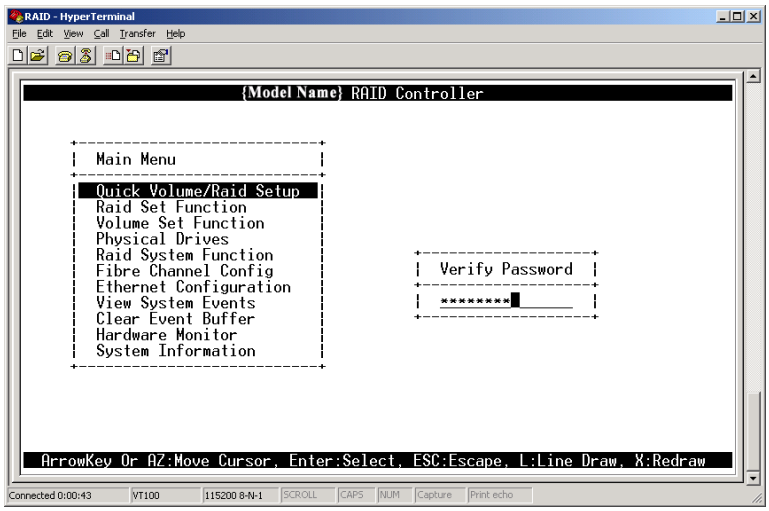
“ESC” key - Return to previous screen

“L” key - Line draw

“X” key – Redraw

Main Menu

The main menu shows all function that enables the customer to execute actions by clicking on the appropriate link.



NOTE: The password option allows user to set or clear the RAID subsystem's password protection feature. Once the password has been set, the user can only monitor and configure the RAID subsystem by providing the correct password. The password is used to protect the RAID subsystem from unauthorized access. The controller will check the password only when entering the Main menu from the initial screen. The RAID subsystem will automatically go back to the initial screen when it does not receive any command in twenty seconds. The RAID subsystem's factory default password is set to 00000000.

VT100 terminal configuration Utility Main Menu Options

Select an option and the related information or submenu items display beneath it. The submenus for each item are shown in Section 4.2.1. The configuration utility main menu options are:

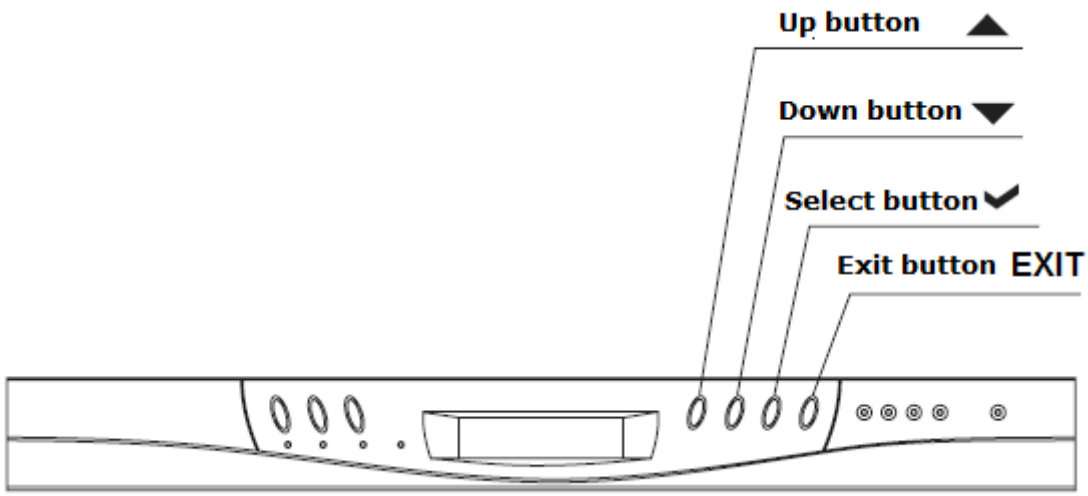
Option	Description
Quick Volume And Raid Set Setup	Create a RAID configuration which consists of all physical disks installed
Raid Set Functions	Create a customized Raid Set
Volume Set Functions	Create a customized Volume Set
Physical Drive Functions	View individual disk information
Raid System Functions	Setting the Raid system configurations
Ethernet Configuration	Setting the Ethernet configurations
Views System Events	Record all system events in the buffer
Clear Event Buffer	Clear all event buffer information
Hardware Monitor	Show all system environment status
System Information	View the controller information

4.2 Configuration through the LCD Panel

All configurations can be performed through the LCD Display front panel function keys, except for the “Firmware update”. The LCD provides a system of screens with areas for information, status indication, or menus. The LCD screen displays menu items or other information up to two lines at a time. The RAID controller’s factory default password is set to **00000000**.

Function Key Definitions

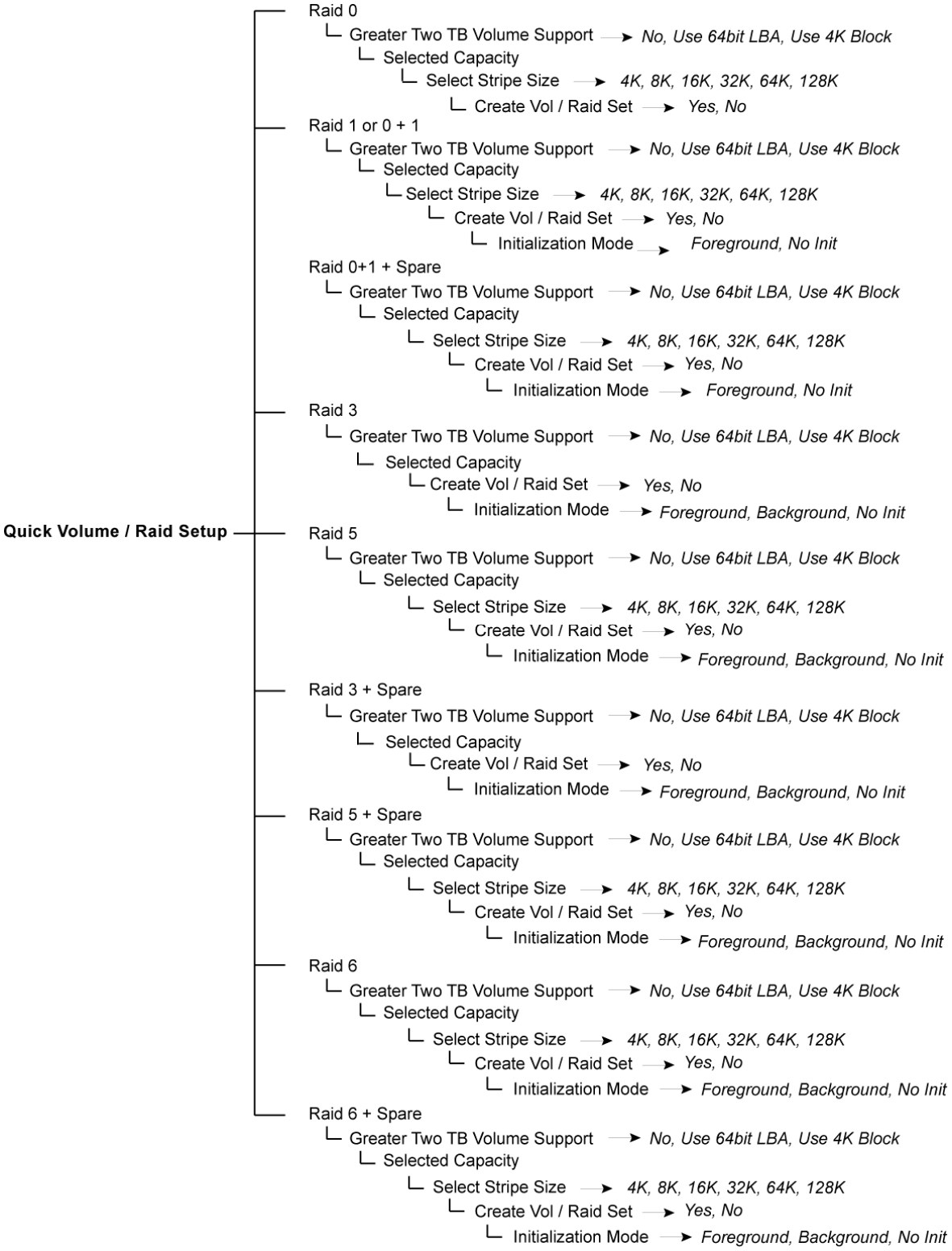
The four function keys at the top of the front panel perform the following functions:

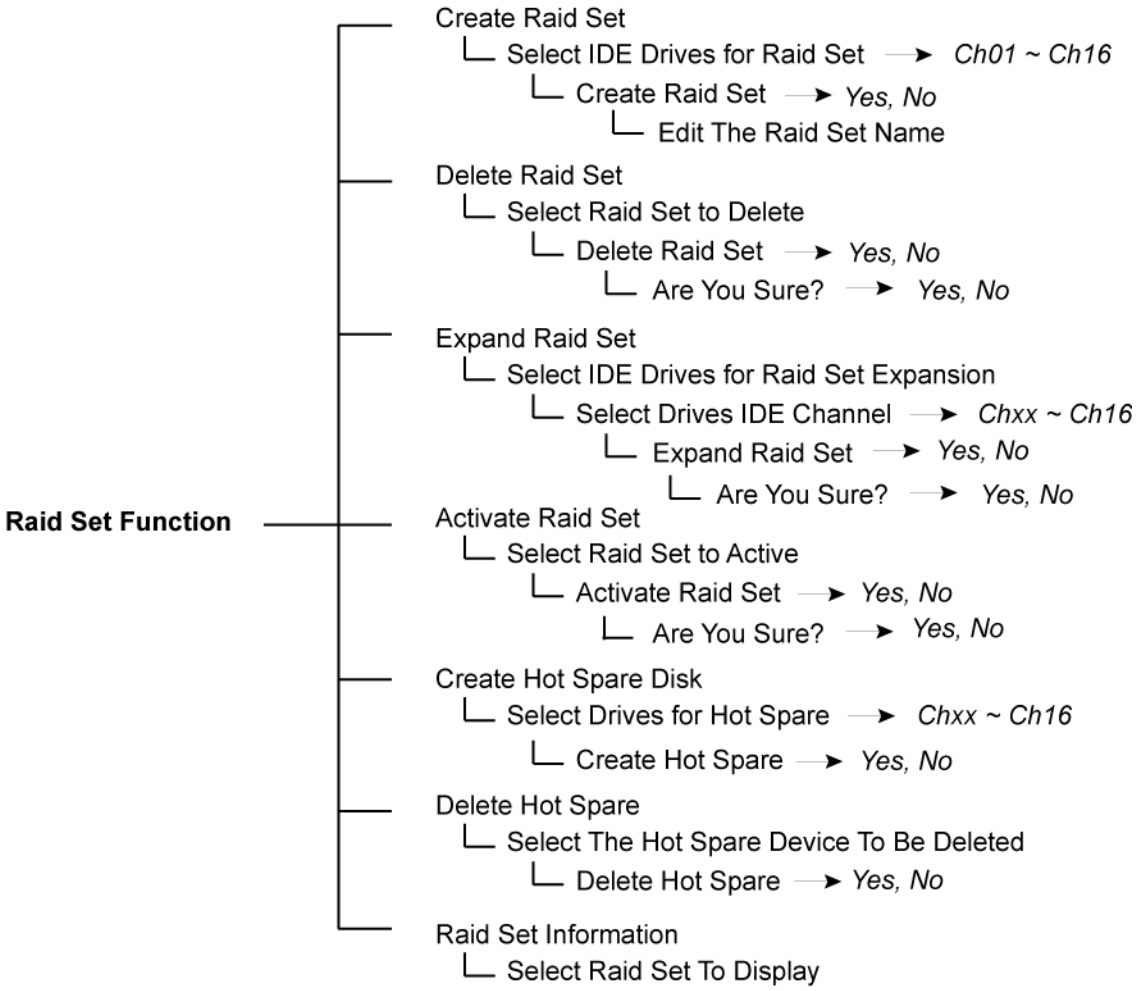


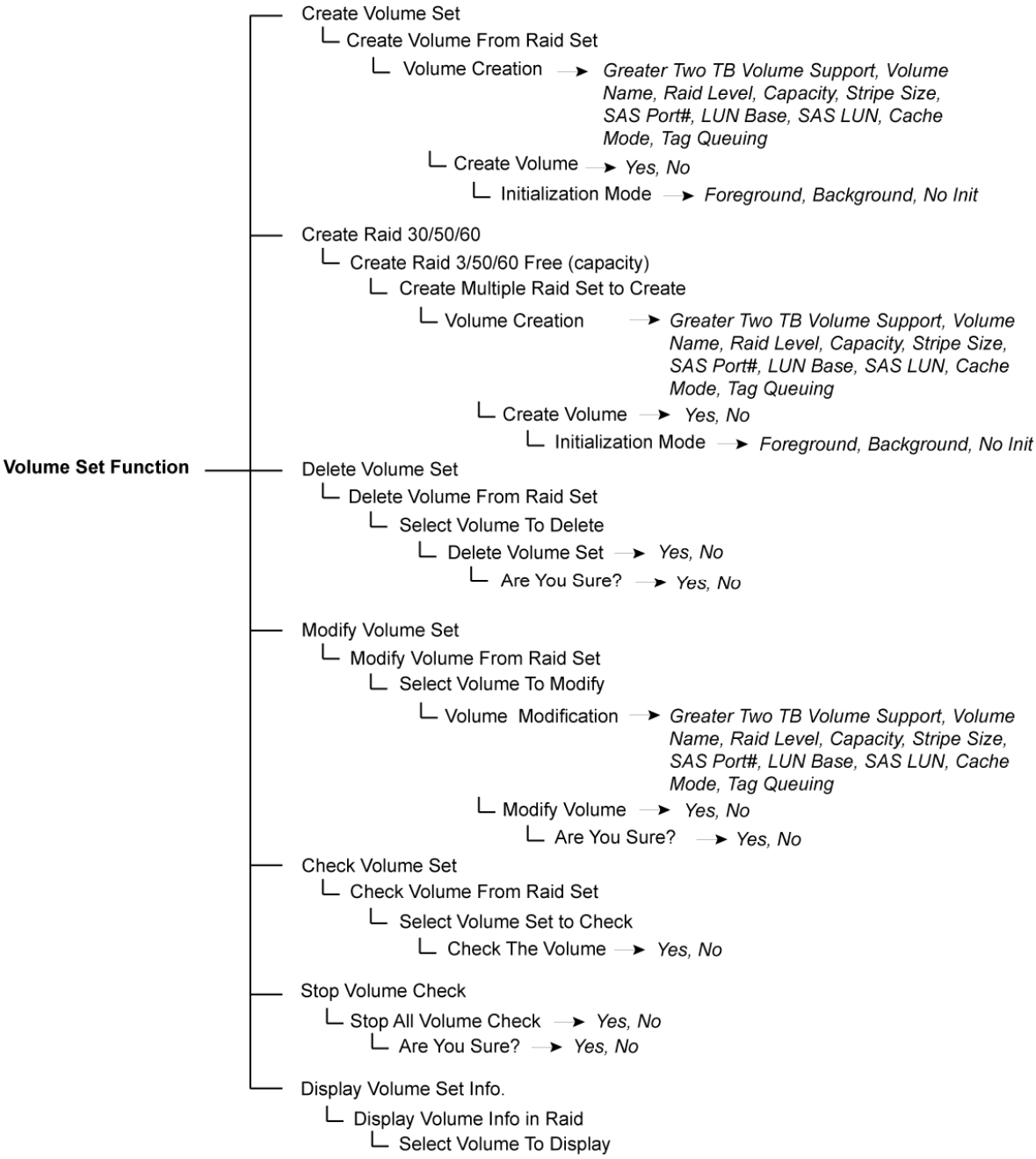
Parts	Function
Up and Down Arrow buttons	Use the Up or Down arrow keys to go through the information on the LCD screen. This is also used to move between each menu when you configure the RAID.
Select button	This is used to enter the option you have selected.
Exit button **EXIT**	Press this button to return to the previous menu. NOTE: This button can also be used to reset the alarm beeper. For example, if one power supply fails, pressing this button will mute the beeper.

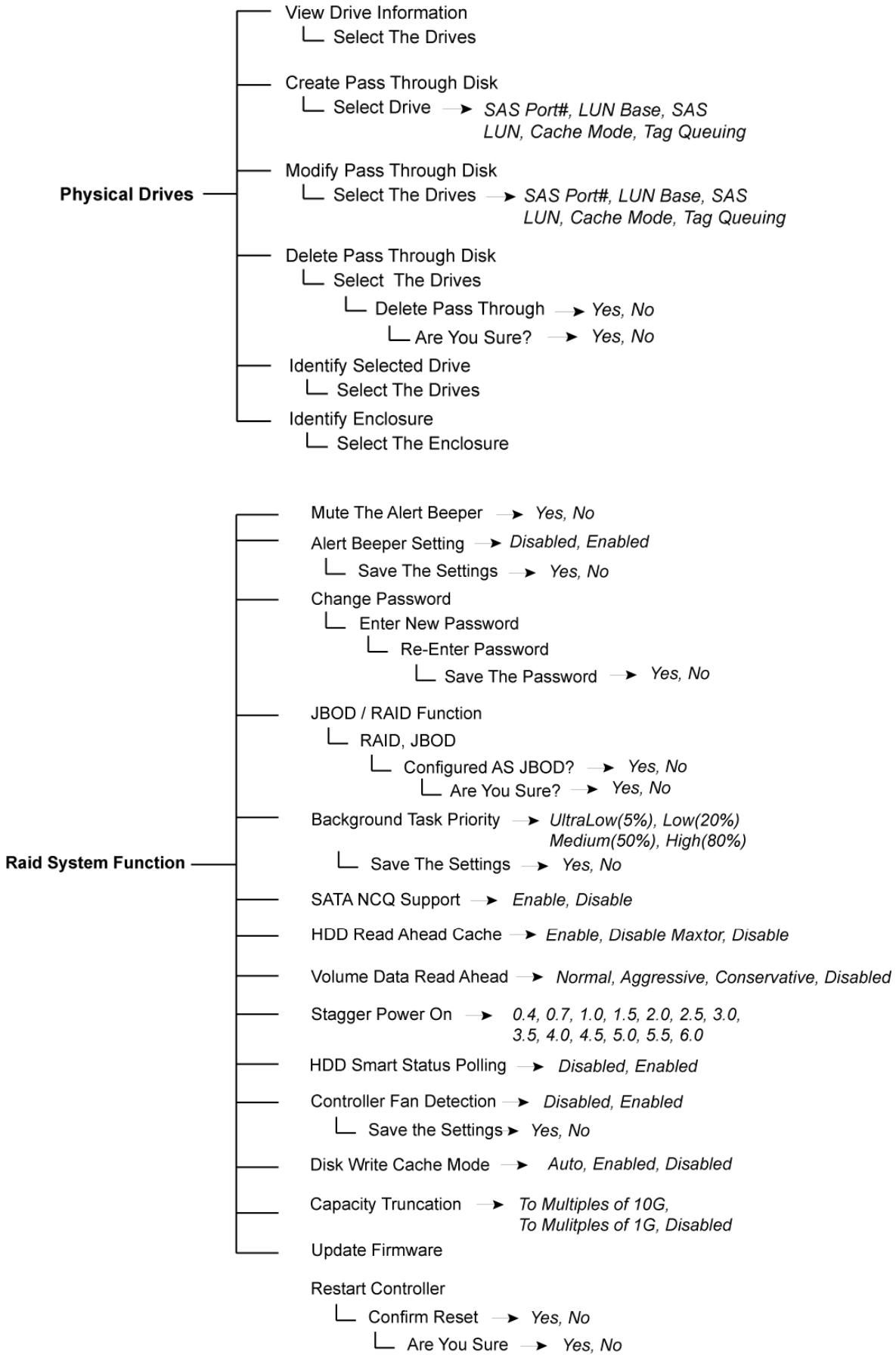
4.2.1 Menu Diagram

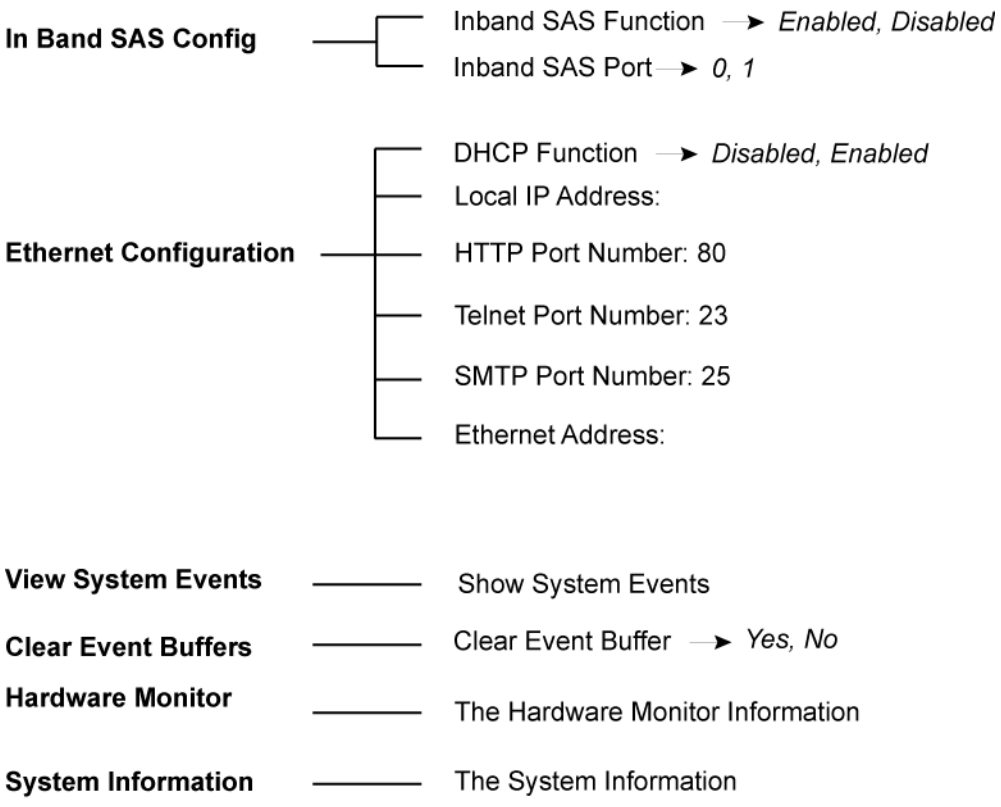
The following menu diagram is a summary of the various configurations and setting functions that can be accessed through terminal. The LCD panel menus also have similar functions except Update Firmware.




Raid Set Function
Create Raid Set
Select IDE Drives for Raid Set → Ch01 ~ Ch16
Create Raid Set → Yes, No
Edit The Raid Set Name
Delete Raid Set
Select Raid Set to Delete
Delete Raid Set → Yes, No
Are You Sure? → Yes, No
Expand Raid Set
Select IDE Drives for Raid Set Expansion
Select Drives IDE Channel → Chxx ~ Ch16
Expand Raid Set → Yes, No
Are You Sure? → Yes, No
Activate Raid Set
Select Raid Set to Active
Activate Raid Set → Yes, No
Are You Sure? → Yes, No
Create Hot Spare Disk
Select Drives for Hot Spare → Chxx ~ Ch16
Create Hot Spare → Yes, No
Delete Hot Spare
Select The Hot Spare Device To Be Deleted
Delete Hot Spare → Yes, No
Raid Set Information
Select Raid Set To Display


Volume Set Function
Create Volume Set
Create Volume From Raid Set
Volume Creation
Greater Two TB Volume Support, Volume Name, Raid Level, Capacity, Stripe Size, SAS Port#, LUN Base, SAS LUN, Cache Mode, Tag Queuing
Create Volume
Yes, No
Initialization Mode
Foreground, Background, No Init
Create Raid 30/50/60
Create Raid 3/50/60 Free (capacity)
Create Multiple Raid Set to Create
Volume Creation
Greater Two TB Volume Support, Volume Name, Raid Level, Capacity, Stripe Size, SAS Port#, LUN Base, SAS LUN, Cache Mode, Tag Queuing
Create Volume
Yes, No
Initialization Mode
Foreground, Background, No Init
Delete Volume Set
Delete Volume From Raid Set
Select Volume To Delete
Delete Volume Set
Yes, No
Are You Sure?
Yes, No
Modify Volume Set
Modify Volume From Raid Set
Select Volume To Modify
Volume Modification
Greater Two TB Volume Support, Volume Name, Raid Level, Capacity, Stripe Size, SAS Port#, LUN Base, SAS LUN, Cache Mode, Tag Queuing
Modify Volume
Yes, No
Are You Sure?
Yes, No
Check Volume Set
Check Volume From Raid Set
Select Volume Set to Check
Check The Volume
Yes, No
Stop Volume Check
Stop All Volume Check
Yes, No
Are You Sure?
Yes, No
Display Volume Set Info.
Display Volume Info in Raid
Select Volume To Display


Physical Drives
View Drive Information
Select The Drives
Create Pass Through Disk
Select Drive
SAS Port#, LUN Base, SAS LUN, Cache Mode, Tag Queuing
Modify Pass Through Disk
Select The Drives
SAS Port#, LUN Base, SAS LUN, Cache Mode, Tag Queuing
Delete Pass Through Disk
Select The Drives
Delete Pass Through
Yes, No
Are You Sure?
Yes, No
Identify Selected Drive
Select The Drives
Identify Enclosure
Select The Enclosure
Raid System Function
Mute The Alert Beeper
Yes, No
Alert Beeper Setting
Disabled, Enabled
Save The Settings
Yes, No
Change Password
Enter New Password
Re-Enter Password
Save The Password
Yes, No
JBOD / RAID Function
RAID, JBOD
Configured AS JBOD?
Yes, No
Are You Sure?
Yes, No
Background Task Priority
UltraLow(5%), Low(20%) Medium(50%), High(80%)
Save The Settings
Yes, No
SATA NCQ Support
Enable, Disable
HDD Read Ahead Cache
Enable, Disable Maxtor, Disable
Volume Data Read Ahead
Normal, Aggressive, Conservative, Disabled
Stagger Power On
0.4, 0.7, 1.0, 1.5, 2.0, 2.5, 3.0, 3.5, 4.0, 4.5, 5.0, 5.5, 6.0
HDD Smart Status Polling
Disabled, Enabled
Controller Fan Detection
Disabled, Enabled
Save the Settings
Yes, No
Disk Write Cache Mode
Auto, Enabled, Disabled
Capacity Truncation
To Multiples of 10G, To Mulitples of 1G, Disabled
Update Firmware
Restart Controller
Confirm Reset
Yes, No
Are You Sure
Yes, No


In Band SAS Config
Inband SAS Function → Enabled, Disabled
Inband SAS Port → 0, 1
Ethernet Configuration
DHCP Function → Disabled, Enabled
Local IP Address:
HTTP Port Number: 80
Telnet Port Number: 23
SMTP Port Number: 25
Ethernet Address:
View System Events
Show System Events
Clear Event Buffers
Clear Event Buffer → Yes, No
Hardware Monitor
The Hardware Monitor Information
System Information
The System Information

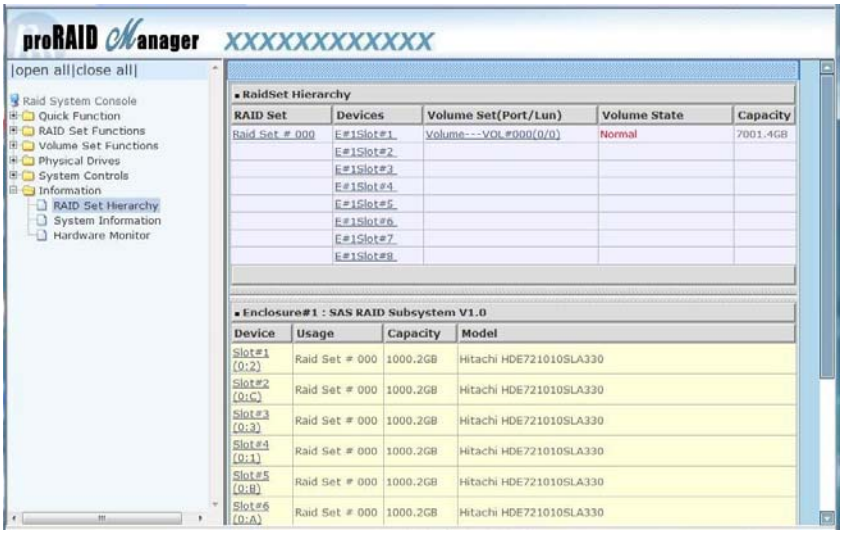
4.3 Configuration through web browser-based proRAID Manager

The RAID subsystem can be remotely configured via R-Link port with proRAID Manager, a web browser-based application. The proRAID Manager can be used to manage all available functions of the RAID controller.

To configure the RAID subsystem from a remote machine, you need to know its IP Address. Launch your web browser from remote machine and enter in the address bar: **http://[IP Address]**.

IMPORTANT! The R-Link default IP Address is 172.16.0.2, subnet mask 255.255.0.0. You can configure the correct IP Address through the LCD panel or the terminal "Ethernet Configuration" menu. The current R-Link IP Address is displayed in the LCD.

Note that you may need to be logged in as administrator with local admin rights on the remote machine to remotely configure the RAID subsystem. The RAID subsystem controller default User Name is "admin" and the Password is "00000000".



Main Menu

The main menu shows all available function that user can execute by clicking on the appropriate hyperlink.

Individual Category	Description
Quick Function	Create a RAID configuration, which consists of all physical disks installed. The Volume Set Capacity, Raid Level, and Stripe Size can be modified during setup.
Raid Set Functions	Create customized Raid Sets.
Volume Set Functions	Create customized Volume Sets and allow modification of parameters of existing Volume Sets parameter.
Physical Drive	Create pass through disks and allow modification of parameters of existing pass through drives. This also provides a function to identify a disk drive.
System Control	For setting the RAID system configurations.
Information	To view the controller and hardware monitor information. The Raid Set hierarchy can also be viewed through the Raid Set Hierarchy item.

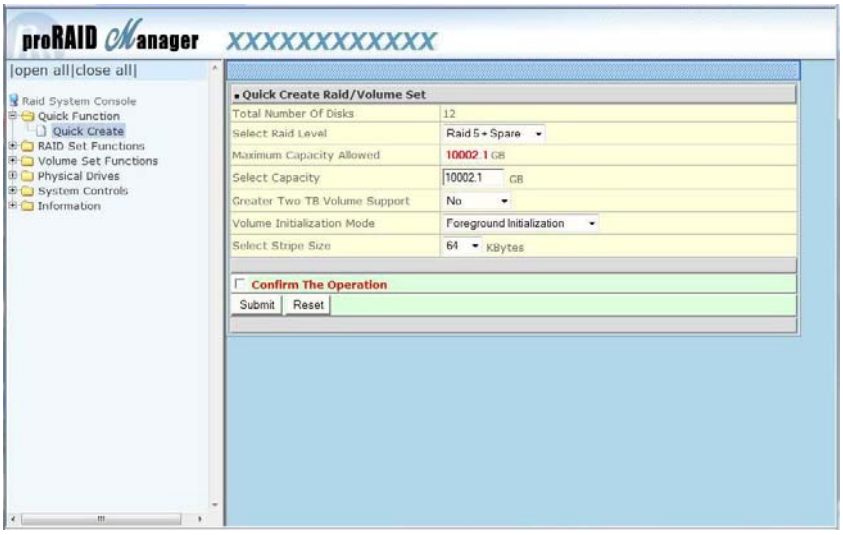
Chapter 5 RAID Management

5.1 Quick Function

5.1.1 Quick Create

The number of physical drives in the RAID subsystem determines the RAID levels that can be implemented with the Raid Set. This feature allows user to create a Raid Set associated with exactly one Volume Set. User can change the Raid Level, Capacity, Volume Initialization Mode and Stripe Size. A hot spare can also be created depending upon the existing configuration.

If the Volume Set size is over 2TB, an option "Greater Two TB Volume Support" will be automatically provided in the screen as shown in the example below. There are three options to select: "No", "64bit LBA", and "4K Block").



Greater Two TB Volume Support:

No: Volume Set capacity is set to maximum 2TB.

64bit LBA: Use this option for UNIX, Linux, and Windows Server 2003 + SP1 or later versions. The maximum Volume Set size is up to 512TB.

4K Block: Use this option for Windows OS such as Windows 2000, 2003, or XP. The maximum Volume Set size is 16TB. Just use the Volume as "Basic Disk". Volume can't be used as "Dynamic Disk"; also can't be used in 512Bytes block service program.

NOTE: For NAS system usage, if you want the maximum capacity allowed to be over 2TB and to have a single Volume Set over 2TB, select the "64bit LBA" option.

Tick on the **Confirm The Operation** option and click on the **Submit** button in the Quick Create screen. The Raid Set and Volume Set will start to initialize.

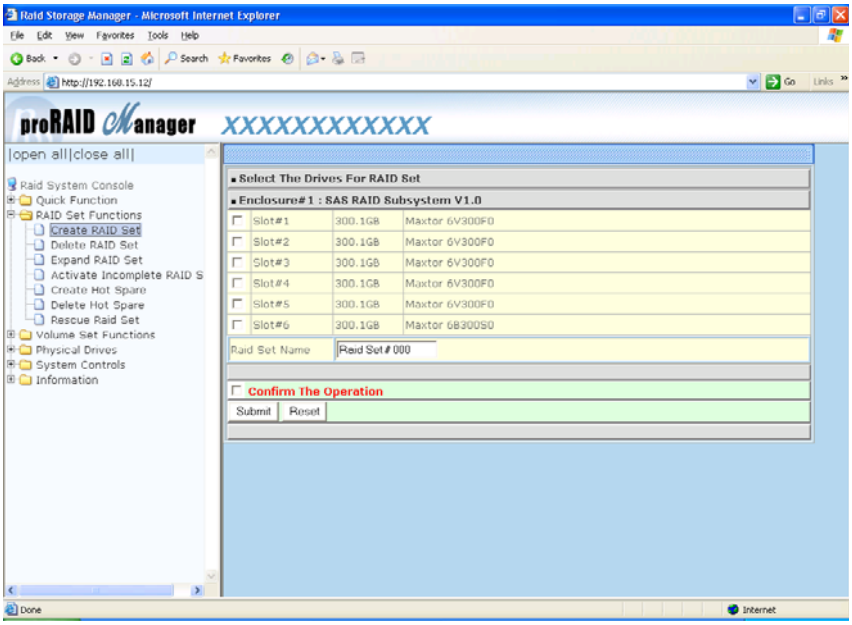
You can use **RaidSet Hierarchy** feature to view the Volume Set information (Refer to Section 5.6.1).

NOTE: In Quick Create your Raid Set is automatically configured based on the number of disks in your system. Use the Raid Set Function and Volume Set Function if you prefer to customize the Raid Set and Volume Set.

5.2 RAID Set Functions

Use the Raid Set Function and Volume Set Function if you prefer to create customized Raid Sets and Volume Sets. User can manually configure and take full control of the Raid Set settings, but it will take a little longer to setup than the Quick Create configuration. Select the Raid Set Function to manually configure the Raid Set for the first time or to delete existing Raid Set and reconfigure a Raid Set.

5.2.1 Create RAID Set



To create a Raid Set, click on the **Create RAID Set** link. A "Select The Drives For RAID Set" screen is displayed showing the disk drives in the system. Tick the box of each disk drive that will be included in Raid Set to be created. Enter the preferred Raid Set Name (1 to 16 alphanumeric characters) to define a unique identifier for the Raid Set. The default Raid Set name will always appear as **Raid Set # xxx**.

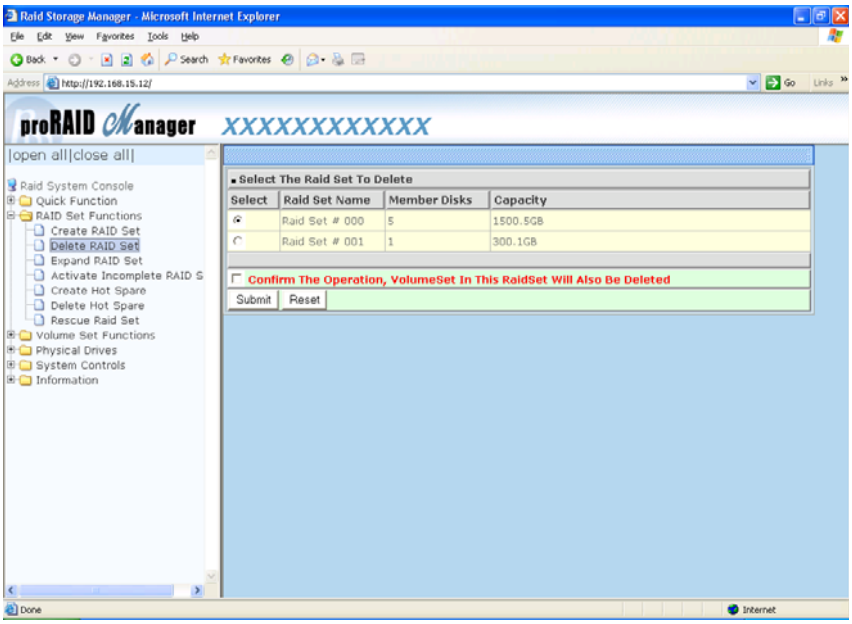
Tick on the **Confirm The Operation** option and click on the **Submit** button in the screen.

NOTE: Maximum number of disk slots supported per RAID Set is 32. For example, you have 16 disk drives in the NAS system, and you connect a SAS JBOD expansion chassis also with 16 disk drives, you can create a single RAID Set using all 32 disk drives.

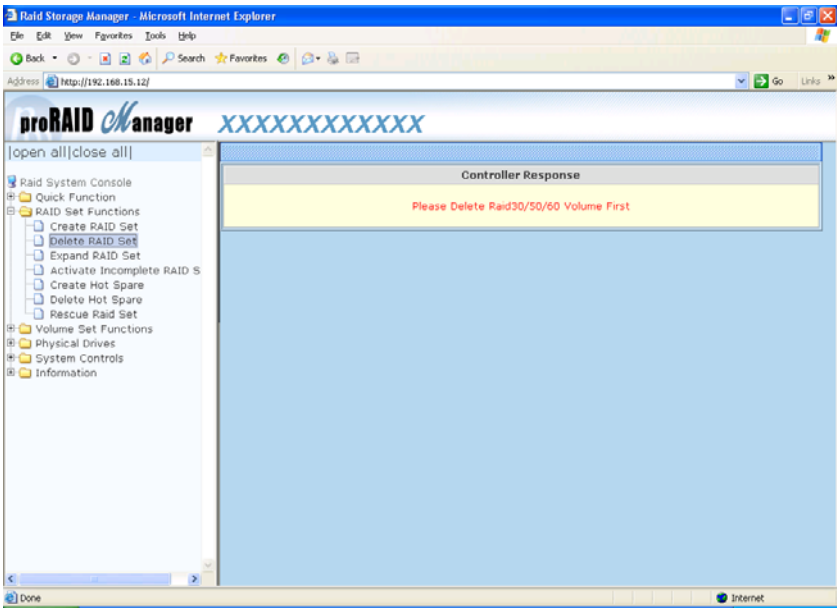
5.2.2 Delete RAID Set

To delete a Raid Set, click on the **Delete RAID Set** link**.** A “Select The RAID SET To Delete” screen is displayed showing all Raid Sets existing in the system. Select the Raid Set you want to delete in the Select column.

Tick on the **Confirm The Operation** and click on the **Submit** button to process with deletion.

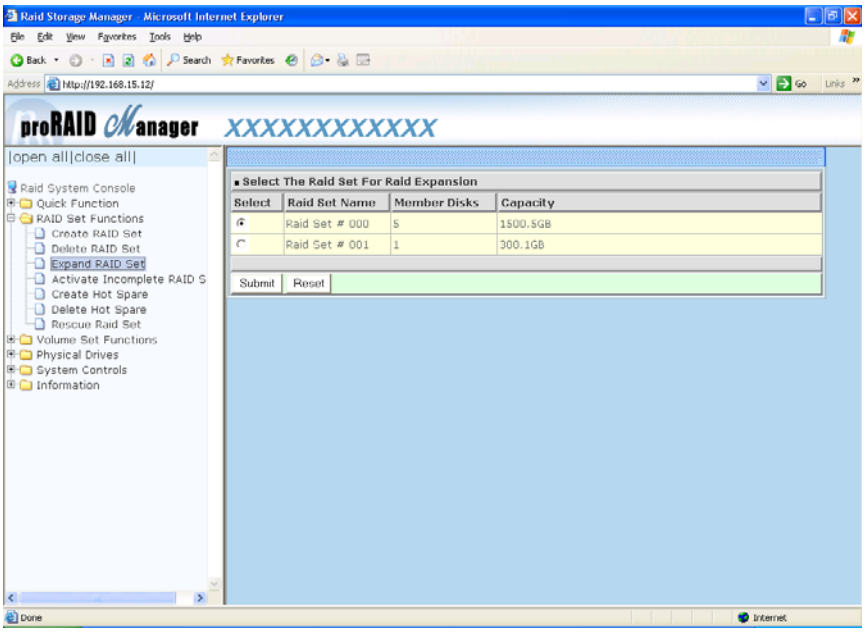


NOTE: You cannot delete a Raid Set containing a Raid 30/50/60 Volume Set. You must delete the Raid 30/50/60 Volume Set first.



5.2.3 Expand RAID Set

Use this option to expand a Raid Set, when one or more disk drives is/are added to the system. This function is active when at least one drive is available.

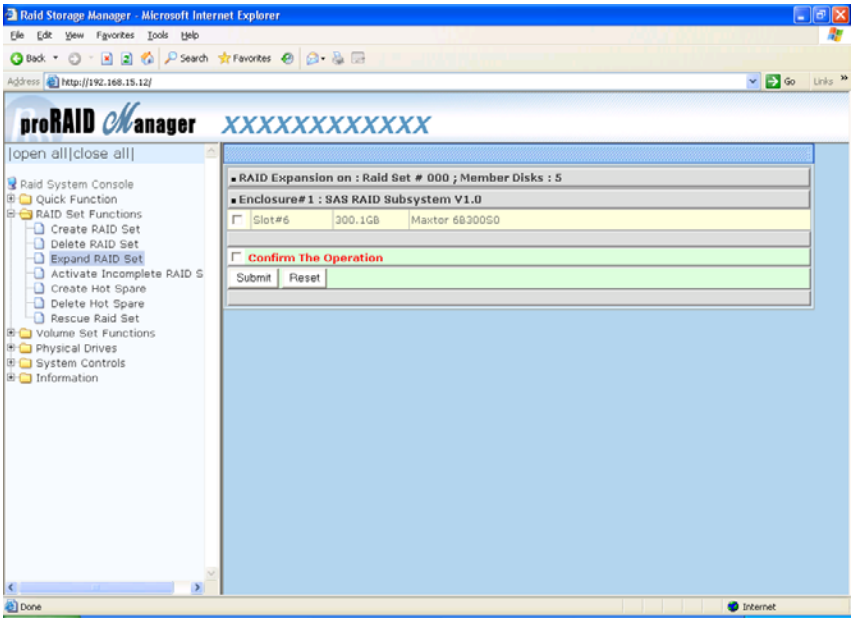


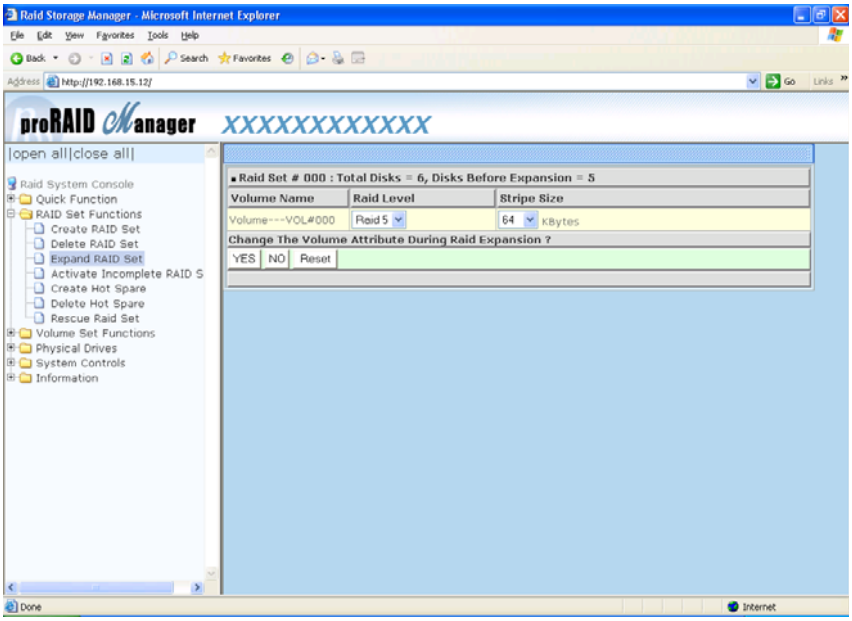
To expand a Raid Set, click on the **Expand RAID Set** link. Select the Raid Set which you want to expand.

Tick on the available disk(s) and check **Confirm The Operation.** Click on the **Submit** button to add the selected disk(s) to the Raid Set.

NOTE: Once the Expand Raid Set process has started, user cannot stop it. The process must be completed.

NOTE: If a disk drive fails during Raid Set expansion and a hot spare is available, an auto rebuild operation will occur after the Raid Set expansion is completed.

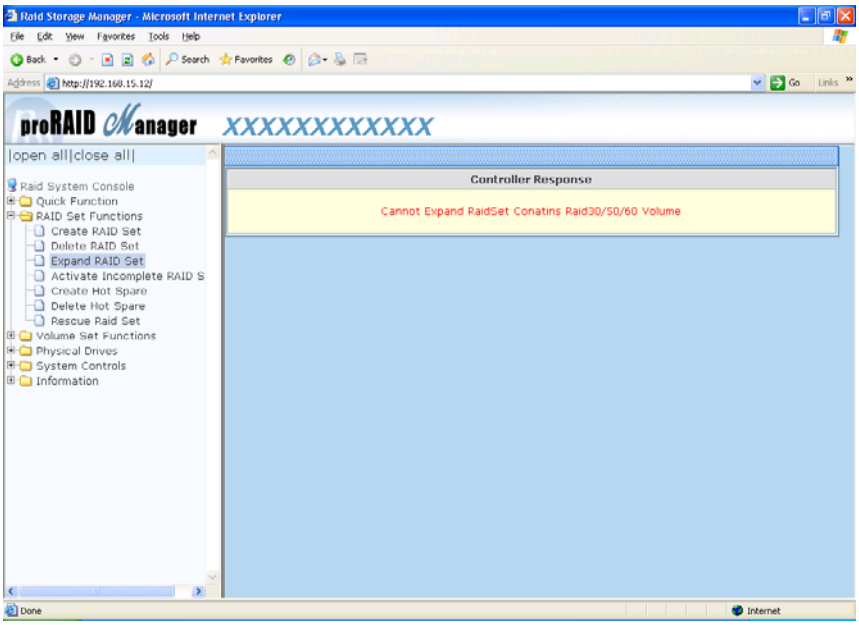




Migration occurs when a disk is added to a Raid Set. Migrating status is displayed in the Raid Set status area of the Raid Set information. Migrating status is also displayed in the Volume Set status area of the Volume Set Information for all Volume Sets under the Raid Set which is migrating.

NOTE: For NAS system usage, after expanding a Raid Set, create a new Volume Set under that Raid Set. The new Volume Set will appear as a new disk device to the NAS system. It is not recommended to expand the capacity of a Volume Set already joined to proNAS Volume Group.

NOTE: A Raid Set cannot be expanded if it contains a Raid 30/50/60 Volume Set.



5.2.4 Offline RAID Set

If it is needed to offline (and move) a Raid Set while the system is powered on, use the Offline Raid Set function. After completing the function, the HDD state will change to "Offlined" Mode and the HDD Status LEDs will be blinking RED.

To offline a Raid Set, click on the **Offline RAID Set** link**.** A "Select The RAID SET To Offline" screen is displayed showing all existing Raid Sets in the subsystem. Select the Raid Set which you want to offline in the Select column.

Tick on the **Confirm The Operation**, and then click on the **Submit** button to offline the selected Raid Set.

IMPORTANT: If the Raid Set/Volume Set is already used by the NAS system (joined to proNAS Volume Group), don't use this function.

5.2.5 Activate Incomplete RAID Set

When Raid Set State is "**Normal**", this means there is no failed disk drive.

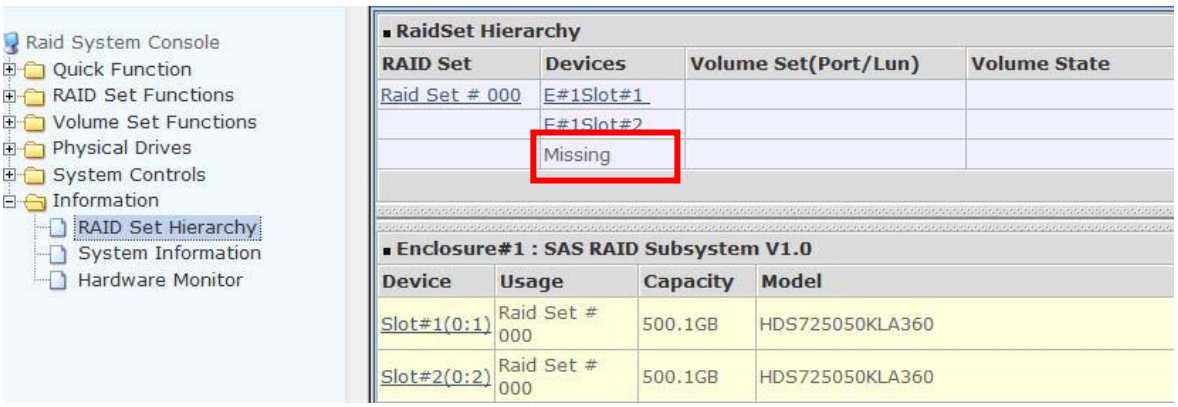
Raid Set Information	
Raid Set Name	Raid Set # 000
Member Disks	3
Total Raw Capacity	247.0GB
Free Raw Capacity	0.0GB
Min Member Disk Size	82.3GB
Raid Set Power State	Operating
Raid Set State	Normal

When does "Incomplete" Raid Set State Happens?

If the RAID controller (and the NAS system) is powered off and one disk drive is removed or has failed in power off state, and when the NAS system is powered on, the Raid Set State will change to "**Incomplete**".

Raid Set Information	
Raid Set Name	Raid Set # 000
Member Disks	3
Total Raw Capacity	247.0GB
Free Raw Capacity	247.0GB
Min Member Disk Size	82.3GB
Raid Set Power State	Operating
Raid Set State	Incomplete

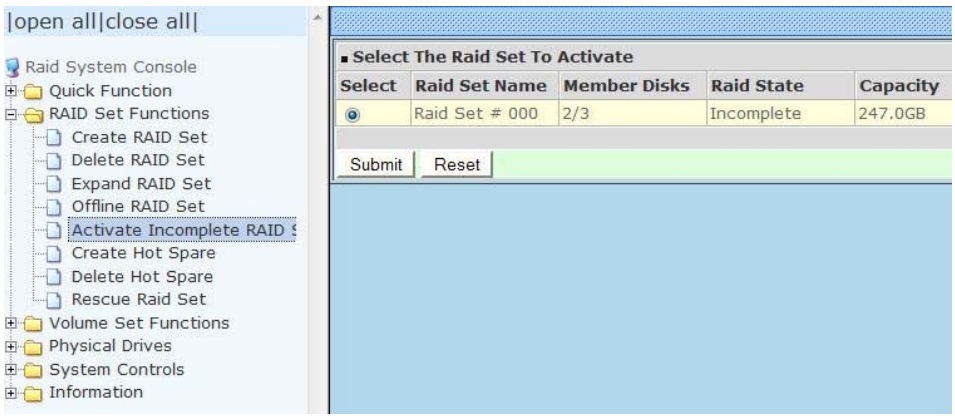
The Volume Set will not be visible and the failed or removed disk will be shown as "**Missing**". At the same time, the NAS system will not detect the Volume Set, hence the NAS volumes are not accessible.



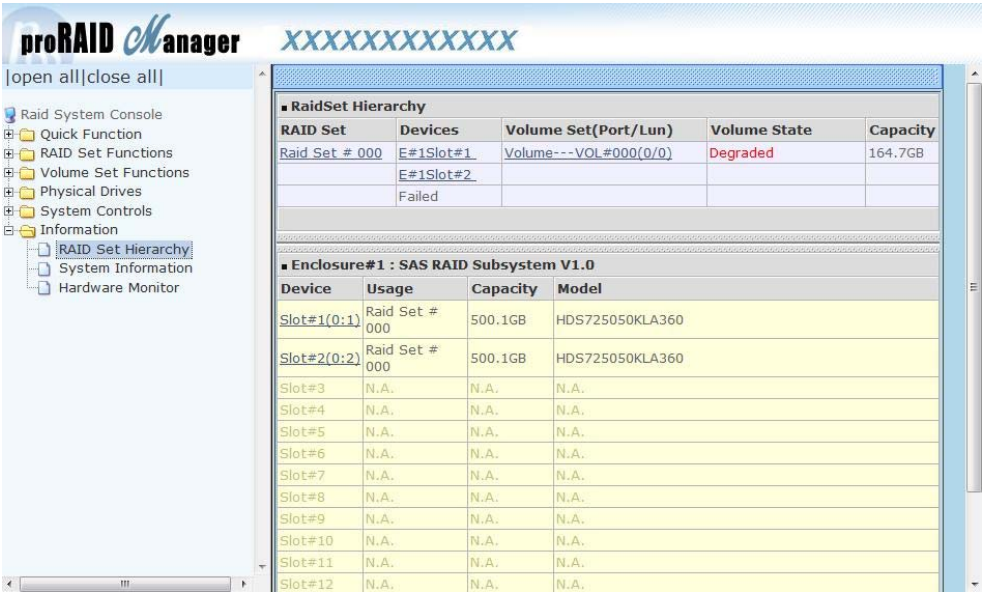
When is the "Activate Raid Set" function can be used?

In order to access the Volume Set and corresponding data, use the **Activate Incomplete RAID Set** function to active the Raid Set. After selecting this function, the Raid State will change to "**Degraded**" state.

To activate the incomplete the Raid Set, click on the **Activate Incomplete RAID Set** link**.** A "Select The Raid Set To Activate" screen is displayed showing all existing Raid Sets in the subsystem. Select the Raid Set with "**Incomplete**" state which you want to activate in the Select column.



Click on the **Submit** button to activate the Raid Set. The Volume Set(s) associated with the Raid Set will become accessible in "**Degraded**" mode.

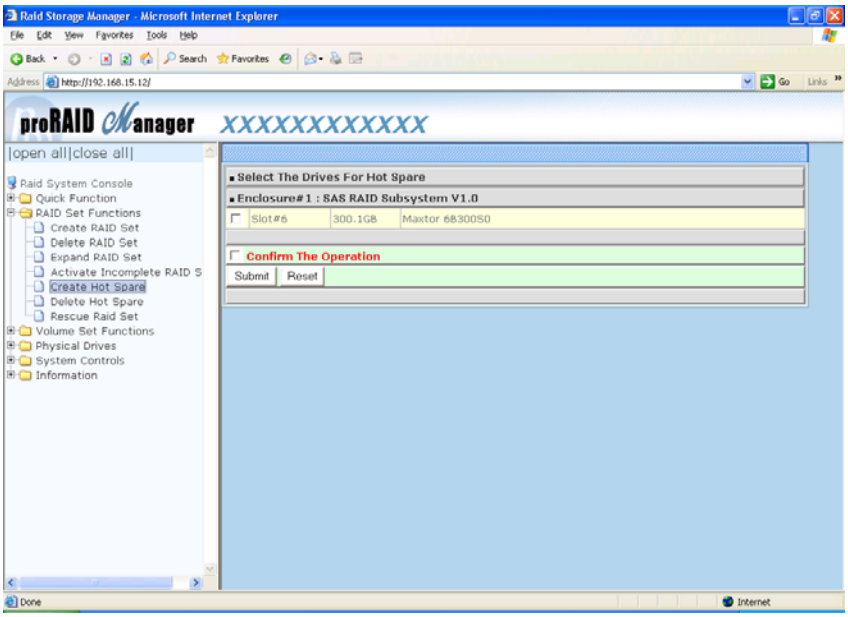


NOTE: The "Activate Raid Set" function is only used when Raid Set State is "Incomplete". It cannot be used when Raid Set configuration is lost. In case the Raid Set configuration is lost, contact your vendor for support.

5.2.6 Create Hot Spare

The Create Hot Spare option gives you the ability to define a global hot spare.

When you choose the **Create Hot Spare** option in the Raid Set Function, all unused (non Raid Set member) disk drives in the subsystem appear. Select the target disk drive by clicking on the appropriate check box. Tick on the **Confirm The Operation** and click on the **Submit** button to create hot spare drive(s).



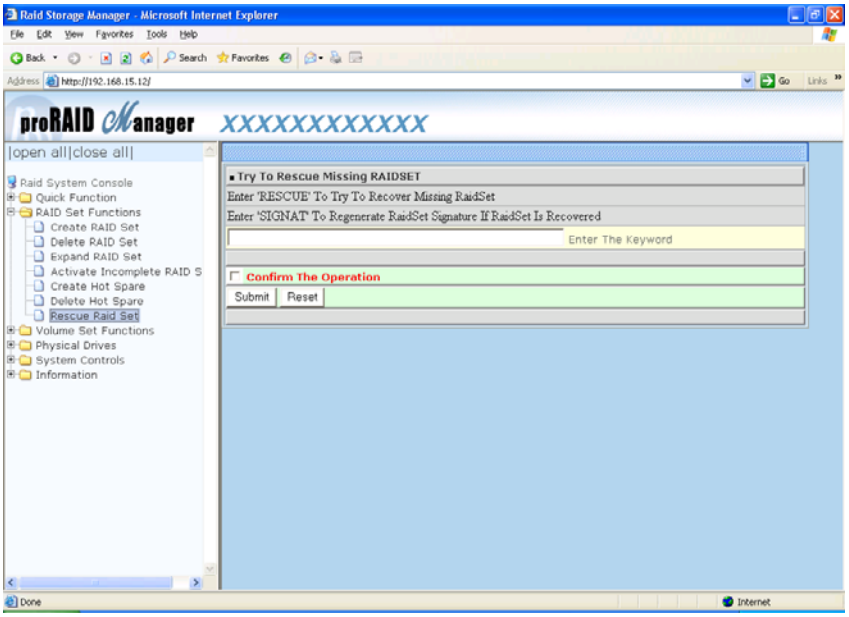
5.2.7 Delete Hot Spare

Select the target Hot Spare disk(s) to delete by clicking on the appropriate check box.

Tick on the **Confirm The Operation**, and click on the **Submit** button in the screen to delete the hot spare(s).

5.2.8 Rescue Raid Set

If you need to recover a missing Raid Set using the “Rescue Raid Set” function, please contact your vendor’s support engineer for assistance.



5.3 Volume Set Function

Volume Set is seen by the host system as a single logical device. It is organized in a RAID level with one or more physical disks. RAID level refers to the level of data performance and protection of a Volume Set. A Volume Set capacity can consume all or a portion of the raw capacity available in a Raid Set. Multiple

Volume Sets can exist on a group of disks in a Raid Set. Additional Volume Sets created in a specified Raid Set will reside on all the physical disks in the Raid Set. Thus each Volume Set on the Raid Set will have its data spread evenly across all the disks in the Raid Set.

5.3.1 Create Volume Set

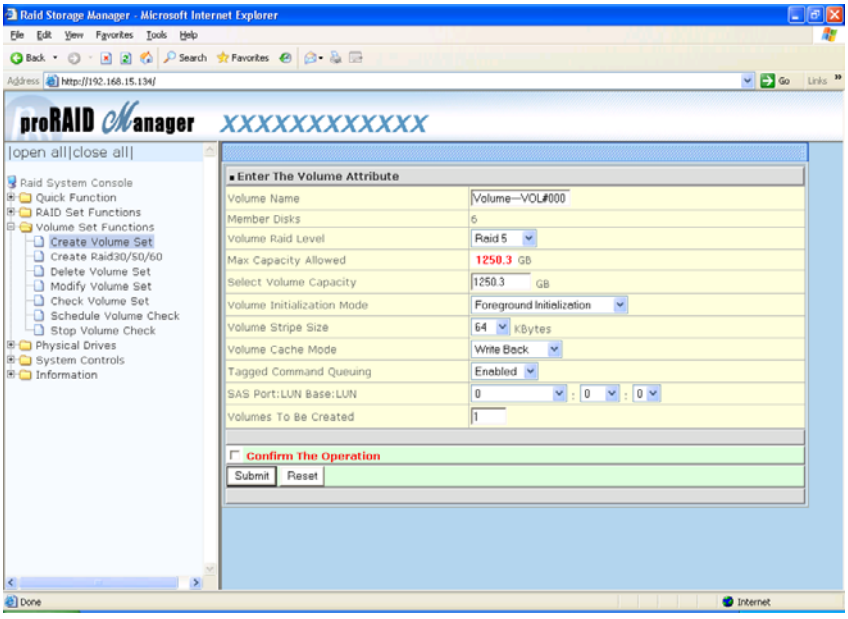
The following are the Volume Set features:

1. Volume sets of different RAID levels may coexist on the same Raid Set.

2. Up to 128 Volume Sets in a Raid Set can be created by the RAID controller.

To create Volume Set from a Raid Set, expand the Volume Set Functions in the main menu and click on the **Create Volume Set** link. The **Select The Raid Set To Create On It** screen will show all existing Raid Sets. Tick on the Raid Set where you want to create the Volume Set and then click on the **Submit** button.

The Volume Set setup screen allows user to configure the Volume Name, Capacity, RAID level, Initialization Mode, Stripe Size, Cache Mode, Tagged Command Queuing, SAS Port/LUN Base/LUN, and Volume To Be Created.



Volume Name:

The default Volume Set name will appear as "Volume---VOL#XXX". You can rename the Volume Set name provided it does not exceed the 16 characters limit.

Raid Level:

Set the RAID level for the Volume Set. Click the down-arrow in the drop-down list. The available RAID levels for the current Volume Set are displayed. Select the preferred RAID level.

Capacity:

The maximum Volume Set size is displayed by default. If necessary, change the Volume Set size appropriate for your application.

Greater Two TB Volume Support:

If the Volume Set size is over 2TB, an option "Greater Two TB Volume Support" will be automatically provided in the screen as shown in the example above. There are three options to select: "No", "64bit LBA", and "4K Block").

No: Volume Set size is set to maximum 2TB limitation.

64bit LBA: Use this option for UNIX, Linux, and Windows Server 2003 + SP1 or later versions. The maximum Volume Set size is up to 512TB.

4K Block: Use this option for Windows OS such as Windows 2000, 2003, or XP. The maximum Volume Set size is 16TB. Just use the Volume as "Basic Disk". Volume can't be used as "Dynamic Disk"; also can't be used in 512Bytes block service program.

NOTE: For NAS system usage, if you want the maximum capacity allowed to be over 2TB and to have a single Volume Set over 2TB, select the "64bit LBA" option.

Initialization Mode:

Set the Initialization Mode for the Volume Set. Foreground mode is completed faster but Volume Set but be completed before it becomes accessible. Background mode makes the Volume Set available instantly but the initialization process takes longer.

Stripe Size:

This parameter sets the size of the stripe written to each disk in a RAID 0, 1, 0+1, 5 or 6 Volume Set. You can set the stripe size to 4 KB, 8 KB, 16 KB, 32 KB, 64 KB, or 128 KB.

A larger stripe size produces better-read performance, especially if your computer does mostly sequential reads. However, if you are sure that your computer does random reads more often, select a small stripe size.

NOTE Stripe Size in RAID level 3 can't be modified.

Cache Mode:

The RAID subsystem supports Write-Through Cache and Write-Back Cache.
Write-Through: the RAID controller acknowledges data has been received when it reaches the disk drives.
Write-Back: the RAID controller acknowledges data has been received when it reaches the controller's cache memory. This provides better performance but requires a battery module support for the cache memory, or a UPS where the system can be connected.

Tagged Command Queuing:

When this option is enabled, it enhances the overall system performance under multi-tasking operating systems by reordering tasks or requests in the command queue of the RAID system. This function should normally remain enabled.

SAS Port/LUN Base/LUN:

SAS Port: There are two 3Gbps SAS Host Channels in the RAID subsystem. Select the SAS port where to map the LUN (Volume Set). Options are: **0**, **1** and **0&1 Cluster**. **0&1 Cluster** will make the LUN visible on both SAS ports.

LUN Base: The base LUN number. Each LUN Base supports 8 LUNs.

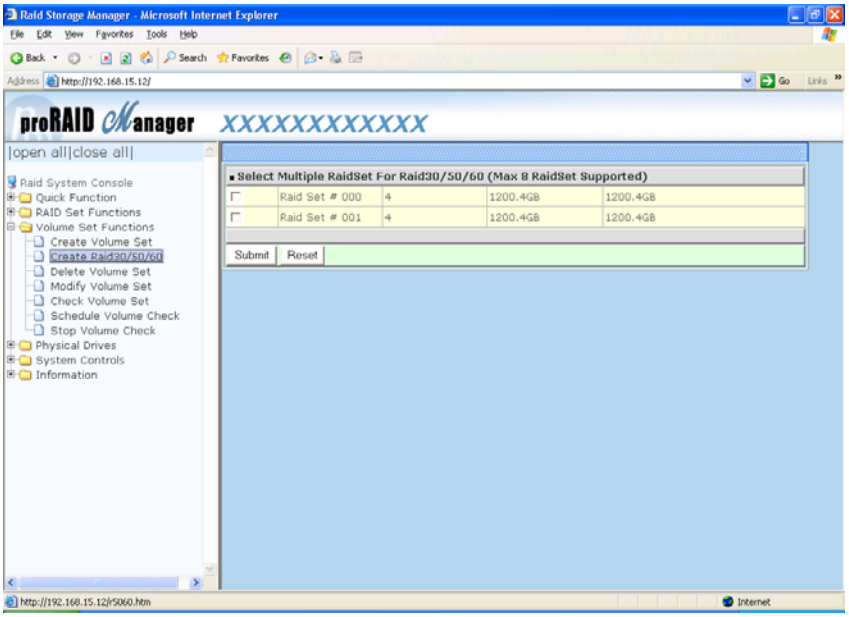
LUN: Each Volume Set must be assigned a unique LUN ID number. A SAS Port can connect up to 128 devices (LUN ID: 0 to 127). Select the LUN ID for the Volume Set.

Volumes To Be Created: Use this option to create several Volume Sets with the same Volume Set attributes. Up to 128 Volume Sets can be created.

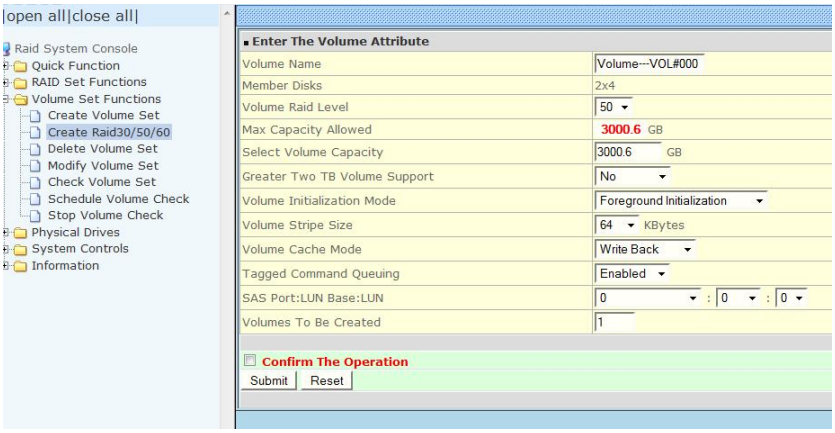
5.3.2 Create Raid 30/50/60

To create a Raid30/50/60 Volume Set, move the mouse cursor to the main menu and click on the **Create Raid30/50/60** link. The **Select Multiple RaidSet For Raid30/50/60** screen will show all Raid Sets. Tick on the Raid Sets that you want to include in the creation and then click on the **Submit** button.

NOTE: The maximum number of Raid Sets supported per RAID controller is 8 (the NAS system contains one RAID controller). All Raid Sets must contain the same number of disk drives.

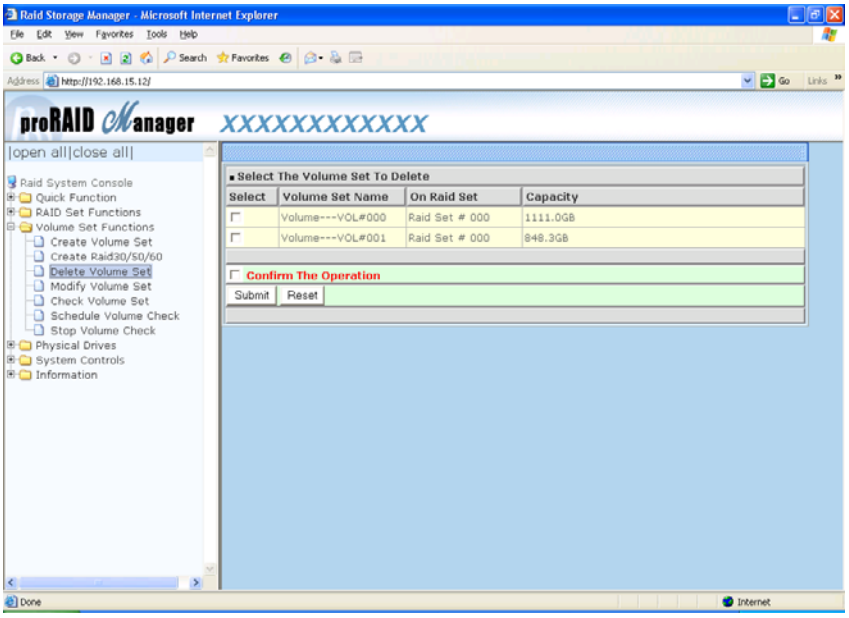


Configure the Volume Set attributes (refer to previous section for the Volume Set attributes). When done, tick **Confirm The Operation** and click on **Submit** button.



5.3.3 Delete Volume Set

To delete a Volume Set, select the Volume Set Functions in the main menu and click on the **Delete Volume Set** link. The **Select The Volume Set To Delete** screen will show all available Raid Sets. Tick on a Raid Set and check the **Confirm The Operation** option and then click on the **Submit** button to show all Volume Sets in the selected Raid Set. Tick on a Volume Set and check the **Confirm The Operation** option. Click on the **Submit** button to delete the Volume Set.



5.3.4 Modify Volume Set

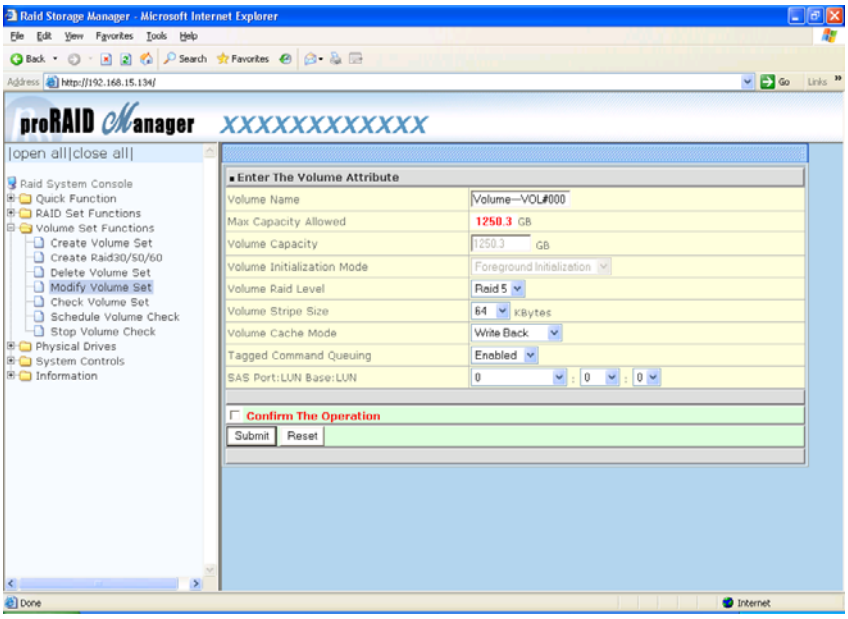
Use this function to modify Volume Set configuration.

To modify the attributes of a Volume Set:

1. Click on the **Modify Volume Set** link.

2. Tick from the list the Volume Set you want to modify. Click on the **Submit** button.

The following screen appears.



To modify Volume Set attribute values, select an attribute item and click on the attribute value. After completing the modification, tick on the **Confirm The Operation** option and click on the **Submit** button to save the changes.

5.3.4.1 Volume Set Expansion

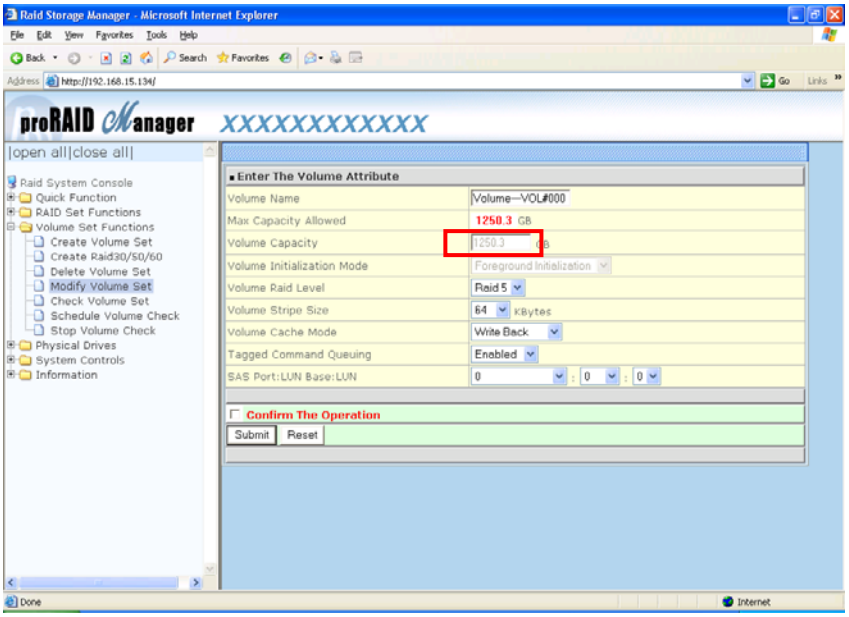
Volume Capacity (Logical Volume Concatenation Plus Re-stripe)

Use the Expand Raid Set function to expand a Raid Set when a disk is added to your subsystem. (Refer to Section 5.2.3)

The expanded capacity can be used to enlarge the Volume Set size or create another Volume Set. Use the Modify Volume Set function to expand the Volume Set capacity. Select the Volume Set and move the cursor to the **Volume Set Capacity** item and enter the capacity size.

NOTE: For NAS system usage, after expanding a Raid Set, create a new Volume Set under that Raid Set. The new Volume Set will appear as a new disk device to the NAS system. It is not recommended to expand the capacity of a Volume Set already joined to proNAS Volume Group.

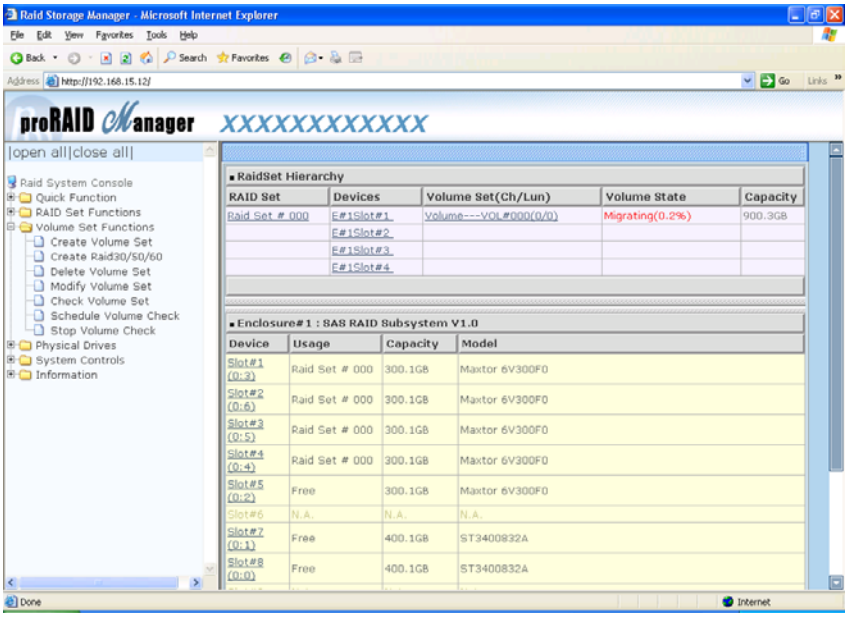
Tick on the **Confirm The Operation** and click on the **Submit** button to complete the action. The Volume Set starts to expand.



NOTE: The Volume Set capacity of Raid30/50/60 cannot be expanded.

5.3.4.2 Volume Set Migration

Migration occurs when a Volume Set migrates from one RAID level to another, a Volume Set stripe size changes, or when a disk is added to a Raid Set. Migrating status is displayed in the Volume Set status area of the RaidSet Hierarchy screen during migration.



NOTE: The Stripe Size of a Raid30 / 50 / 60 Volume Set cannot be modified.

5.3.5 Check Volume Set

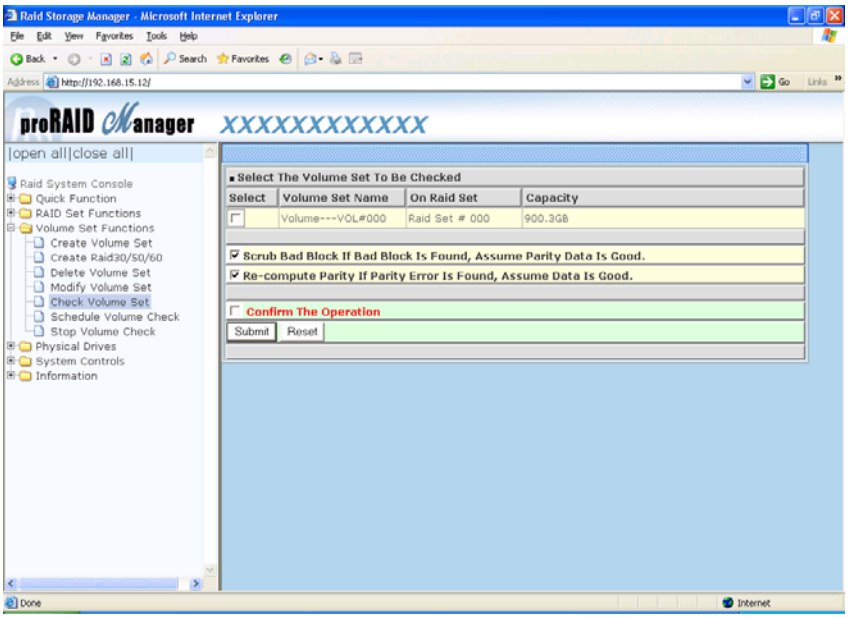
Use this function to perform Volume Set consistency check, which verifies the correctness of redundant data (data blocks and parity blocks) in a Volume Set. This basically means computing the parity from the data blocks and comparing the results to the contents of the parity blocks, or computing the data from the parity blocks and comparing the results to the contents of the data blocks.

NOTE: The Volume Set state must be Normal in order to perform Check Volume Set. Only RAID levels with parity (redundant data) such as RAID Levels 3, 5, 6, 30, 50 and 60 support this function.

To perform Check Volume Set function:

1. Click on the **Check Volume Set** link.

2. Tick from the list the Volume Set you want to check. Select the Check Volume Set options.



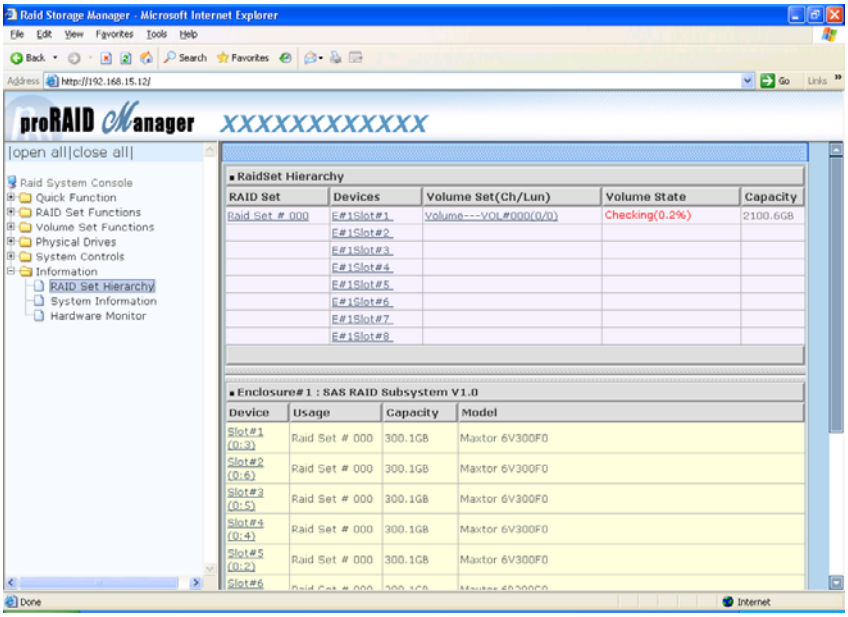
Check Volume Set Options:

- **Scrub Bad Block If Bad Block Found, Assume Parity Data is Good**
- **Re-compute Parity if Parity Error, Assume Data is Good**

NOTE: When the 2 options are not selected, it will only check for errors. It is recommended to perform Check Volume Set with the 2 options unselected at first. If the result shows error, the two options can be selected and redo Check Volume Set to correct the errors.

3. Tick on **Confirm The Operation** and click on the **Submit** button. The Checking process will be started.

The checking percentage can also be viewed by clicking on RaidSet Hierarchy in the Information menu.



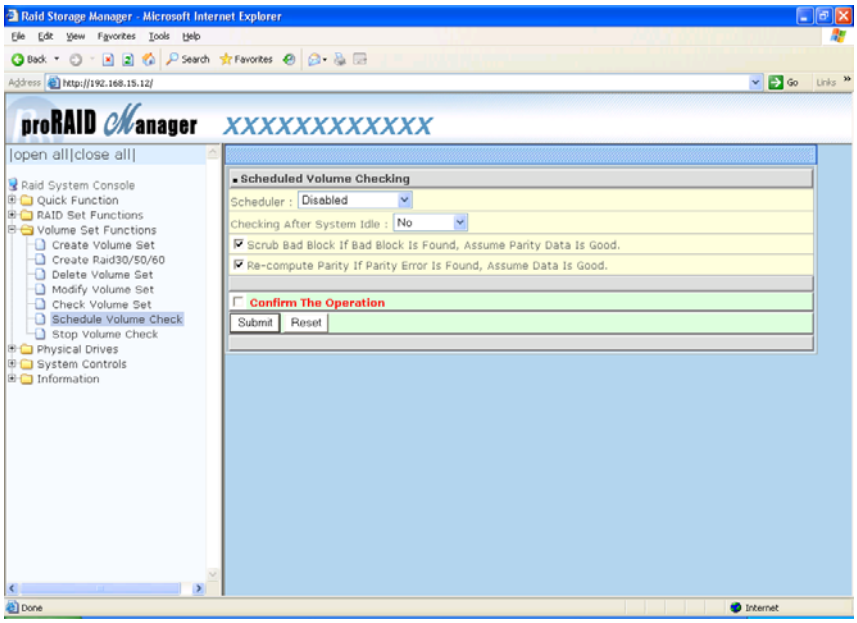
5.3.6 Schedule Volume Check

To perform Check Volume Set by schedule, follow these steps:

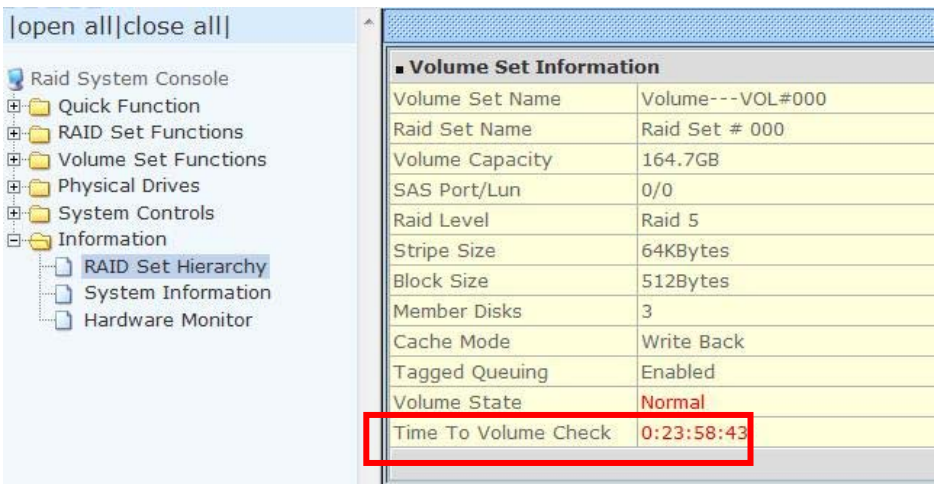
1. Click on the **Schedule Volume Check** link.
2. Select the desired schedule that you wish the Check Volume Set function to run. Tick on **Confirm The Operation** and click on the **Submit** button.

Scheduler: Disabled, 1Day (For Testing), 1Week, 2Weeks, 3Weeks, 4Weeks, 8Weeks, 12Weeks, 16Weeks, 20Weeks and 24Weeks.

Check After System Idle: No, 1 Minute, 3 Minutes, 5 Minutes, 10 Minutes, 15 Minutes, 20 Minutes, 30 Minutes, 45 Minutes and 60 Minutes.



NOTE: To verify the Volume Check schedule, go to Information -> RAID Set Hierarchy -> select the Volume Set -> the Volume Set Information will be displayed.



5.3.7 Stop Volume Check

Use this option to stop current running Check Volume Set process.

5.4 Physical Drive

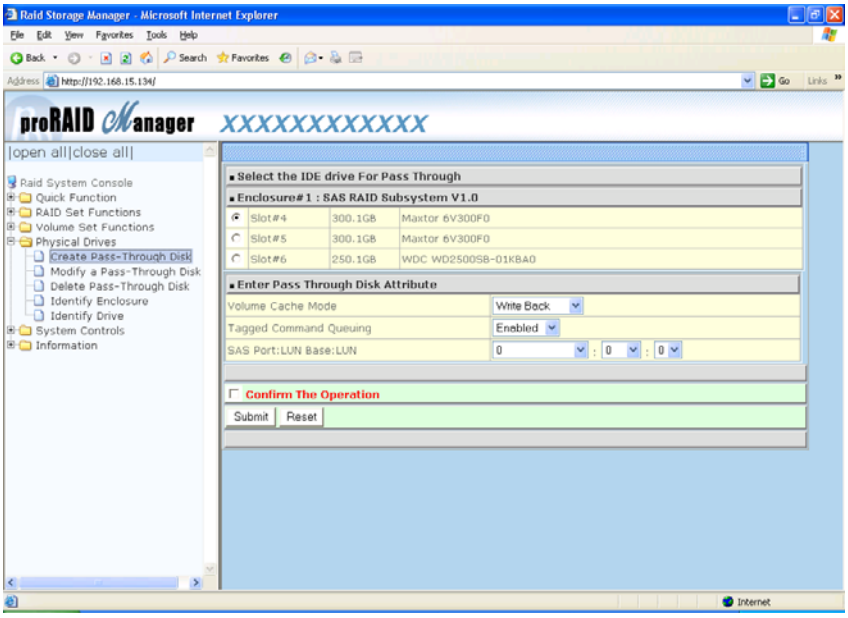
Choose this option from the Main Menu to select a disk drive and to perform the functions listed below.

5.4.1 Create Pass-Through Disk

A Pass-Through Disk is a disk drive not controlled by the internal RAID subsystem firmware and thus cannot be a part of a Volume Set. A Pass-Through disk is a separate and individual Raid Set. The disk is available to the host as an individual disk. It is typically used on a system where the operating system is on a disk not controlled by the RAID firmware.

To create pass-through disk, click on the **Create Pass-Through** link under the Physical Drives main menu. The setting function screen appears.

Select the disk drive to be made as Pass-Through Disk and configure the Pass-Through Disk attributes, such as the Cache Mode, Tagged Command Queuing, and SAS Port/LUN Base/LUN for this volume.

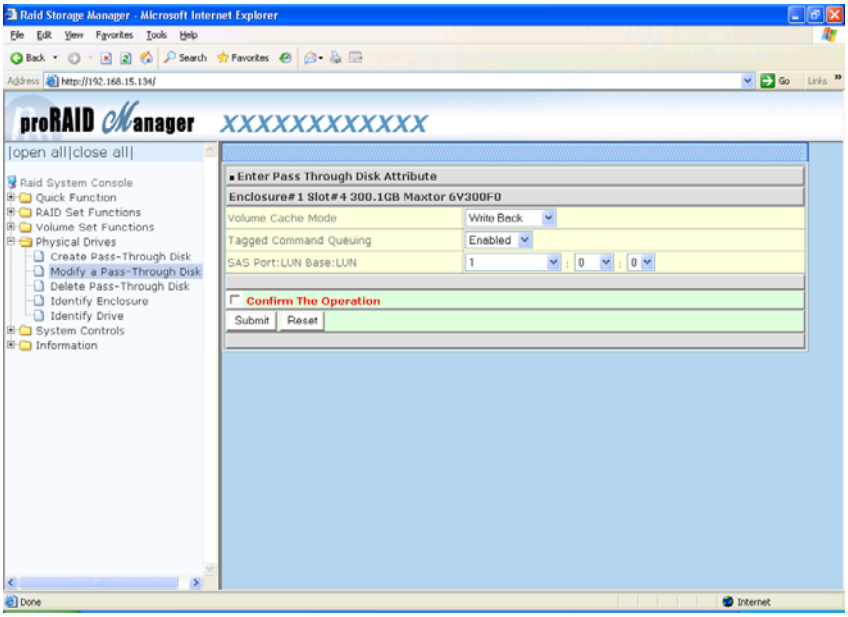


5.4.2 Modify a Pass-Through Disk

Use this option to modify the attribute of a Pass-Through Disk. User can modify the Cache Mode, Tagged Command Queuing, and SAS Port/LUN Base/LUN on an existing Pass-Through Disk.

To modify the Pass-Through drive attribute from the Pass-Through drive pool, click on the **Modify a Pass-Through Disk** link. The "Select The Pass-Through Disk For Modification" screen appears. Tick on the Pass-Through Disk from the Pass-Through drive pool and click on the **Submit** button to select the drive.

The Enter Pass-Through Disk Attribute screen appears. Modify the drive attribute values as you want.

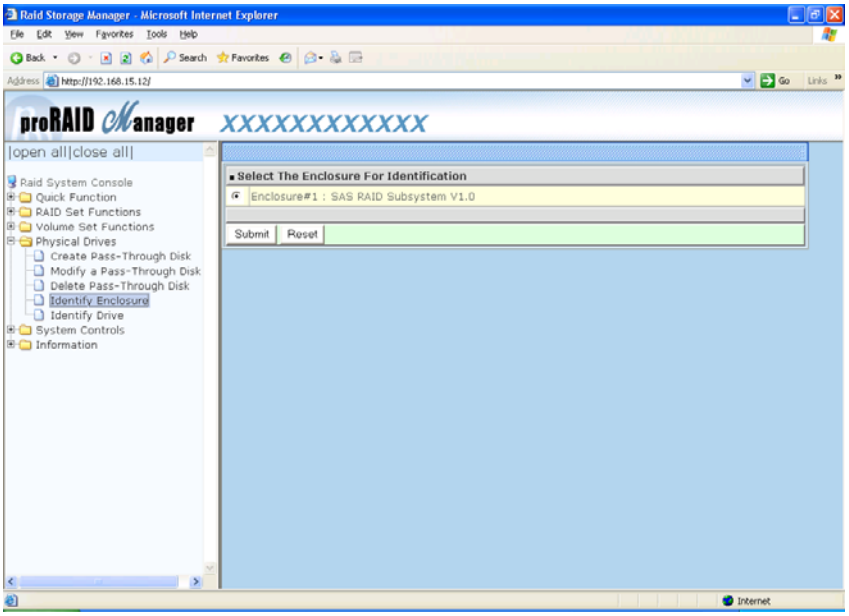


5.4.3 Delete Pass-Through Disk

To delete Pass-Through Disk from the Pass-Through drive pool, click on **Delete Pass-Through** link. Select a Pass-Through Disk, tick on the **Confirm The Operation** and click the **Submit** button to complete the delete action.

5.4.4 Identify Enclosure

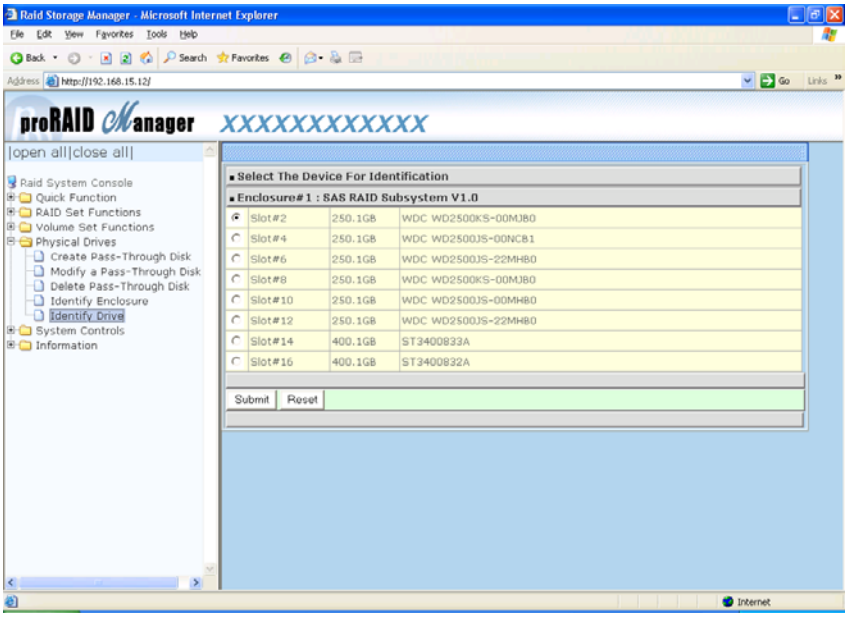
To identify an Enclosure, move the mouse cursor and click on **Identify Enclosure** link. The **Select The Enclosure For Identification** screen appears. Tick on the enclosure from the list of enclosures, then click on the **Submit** button to identify the selected enclosure. All disk drives' LEDs in an enclosure will flash when a particular enclosure is selected.



5.4.5 Identify Selected Drive

Use this option to physically locate a selected drive to prevent removing the wrong drive. When a disk drive is selected using the **Identify Drive** function, the Status LED of the selected disk drive will be blinking.

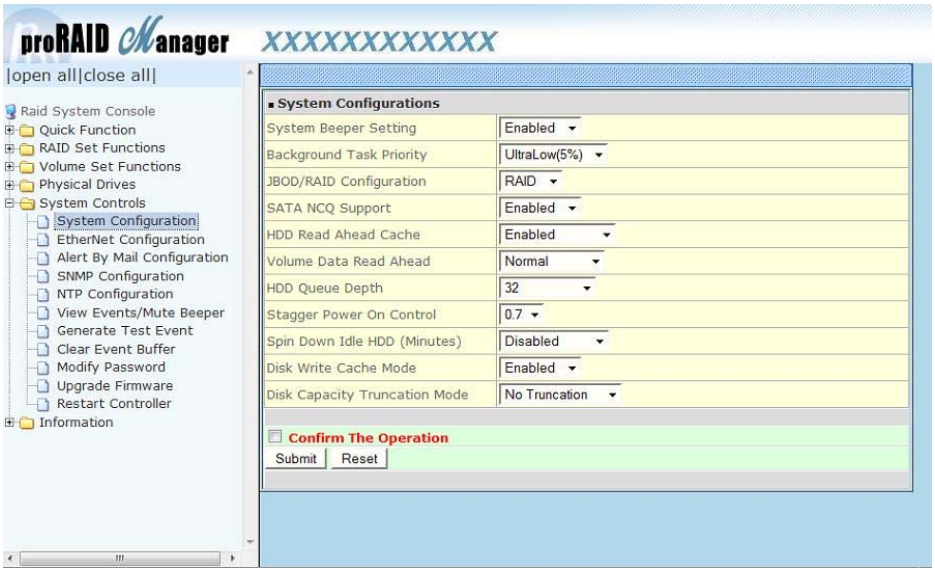
To identify a selected drive from the drives pool, click on the **Identify Drive** link. The "Select The IDE Device For identification" screen appears. Tick on the IDE device from the drives list. After completing the selection, click on the **Submit** button to identify selected drive.



5.5 System Controls

5.5.1 System Configuration

To set the RAID subsystem system configuration options, click the **System Configuration** link under the **System Controls** menu. The System Configurations screen will be shown. Set the desired system option as needed.



System Beeper Setting:

This option is used to Disable or Enable the system's RAID controller alarm beeper.

Background Task Priority:

The Background Task Priority indicates how much time and system resource the RAID controller devotes to a background task, such as a rebuild operation. The RAID subsystem allows user to choose the background task priority (High 80%, Medium 50%, Low 25%, and Ultra Low 5%) to balance between background task process and Volume Set access. For high RAID subsystem performance, specify a low value.

JBOD/RAID Configuration:

The RAID subsystem supports JBOD and RAID configuration.

SATA NCQ Support:

NCQ is a command protocol in Serial ATA that can only be implemented on native Serial ATA hard drives. It allows multiple commands to be outstanding within a drive at the same time. Drives that support NCQ have an internal queue where outstanding commands can be dynamically rescheduled or re-ordered, along with the necessary tracking mechanisms for outstanding and completed portions of the workload. Disabled or Enable the SATA NCQ function.

HDD Read Ahead Cache:

This option allows the users to disable the cache of the HDDs on the RAID subsystem. In some HDD models, disabling the cache in the HDD is necessary to prove the RAID subsystem functions correctly.

Volume Data Read Ahead:

This option allows the users to set the Volume Data Read Ahead function. Options are: Normal, Aggressive, Conservative, and Disabled.

HDD Queue Depth:

The queue depth is the number of I/O operations that can be run in parallel on a disk drive. HDD Queue Depth options are 1, 2, 4, 8, 16, and 32.

Stagger Power On Control:

This option allows the RAID subsystem's power supply to power up in succession each HDD in the RAID subsystem. In the past, all the HDDs on the RAID subsystem are powered up altogether at the same time. This function allows the power transfer time (lag time) from the last HDD to the next one be set within the range of 0.4 to 6.0 seconds.

Spin Down Idle HDD (Minutes):

This option enables the hard drives to spin down after they become idle after a preset period of time. Options are: Disabled, 1 (For Test), 3, 5, 10, 15, 20, 30, 40, and 60.

Disk Write Cache Mode:

The RAID subsystem supports Disk Write Cache Mode options: Auto, Enabled, and Disabled. If the RAID subsystem has BBM (battery backup module), selecting the Auto option will automatically enable Disk Write Cache. On the other hand, if there is no BBM, the Auto option will disable Disk Write Cache.

Disk Capacity Truncation Mode:

The RAID subsystem use drive truncation so that drives from different vendors are more likely to be able to be used as spares for each other. Drive truncation slightly decreases the usable capacity of a drive that is used in redundant units. Options are:

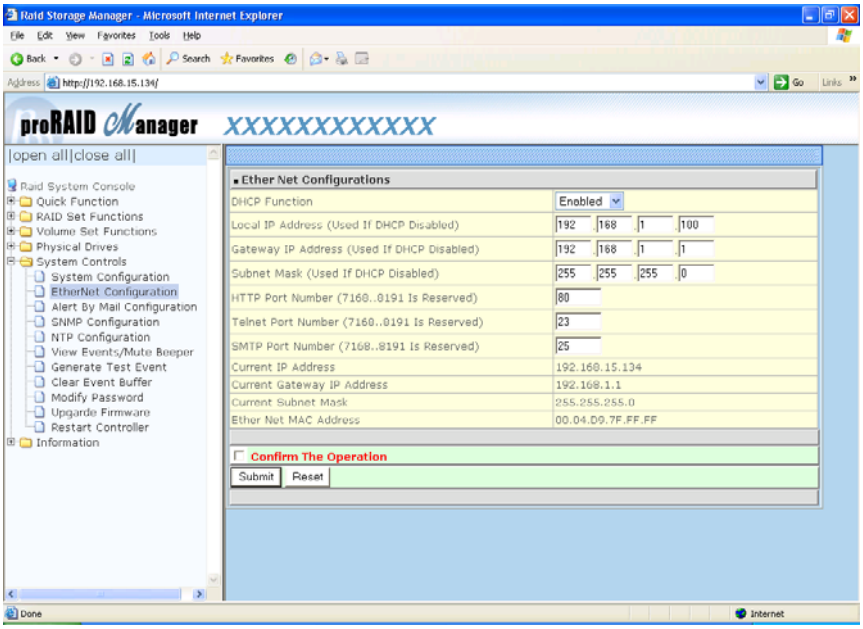
Multiples Of 10G: If you have several 120GB drives from different vendors, chances are that the capacity varies slightly. For example, one drive might be 121.1 GB, and the other 120.4 GB. This drive truncation mode makes the 121.1 GB and 120.4 GB drives same capacity as 120 GB so that one could replace the other.

Multiples Of 1G: If you have 120 GB drives from different vendors, chances are that the capacity varies slightly. For example, one drive might be 121.1 GB, and the other 121.4 GB. This drive truncation mode makes the 121.1 GB and 121.4 GB drives same capacity 121 GB so that one could replace the other.

No Truncation: The capacity of the disk drive is not truncated.

5.5.2 EtherNet Configuration

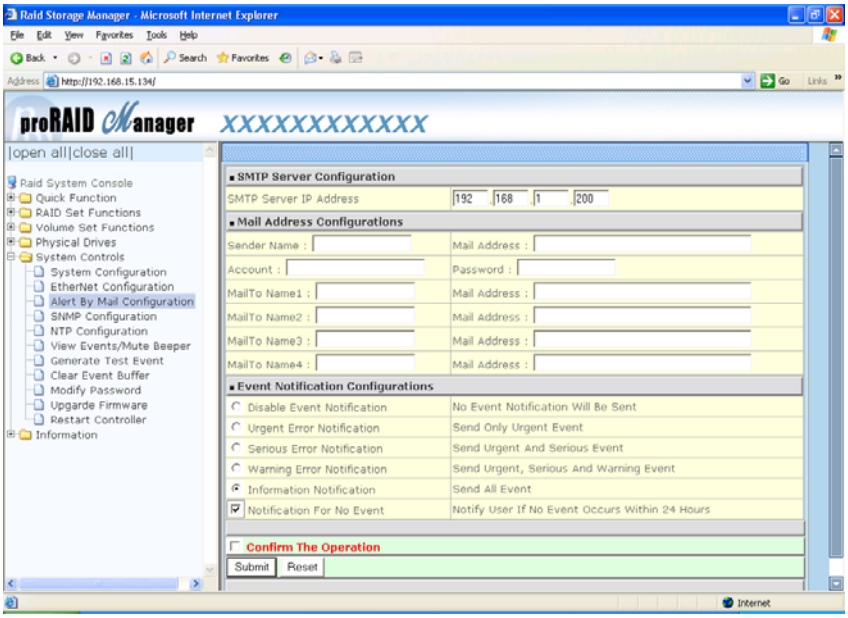
To set the Ethernet configuration, click the **EtherNet Configuration** link under the System Controls menu. The RAID subsystem EtherNet Configuration screen will be shown. Set the desired configuration. Once done, tick on the **Confirm The Operation** and click the **Submit** button to save the settings.



NOTE: If HTTP, Telnet and SMTP Port Number is set to "0", the service is disabled.

5.5.3 Alert By Mail Configuration

To set the Event Notification function, click on the **Alert By Mail Configuration** link under the System Controls menu. The RAID subsystem Event Notification configuration screen will be shown. Set up the desired function and option. When an abnormal condition occurs, an error message will be emailed to the email recipient(s) that a problem has occurred. Events are classified into 4 levels (Urgent, Serious, Warning, and Message).

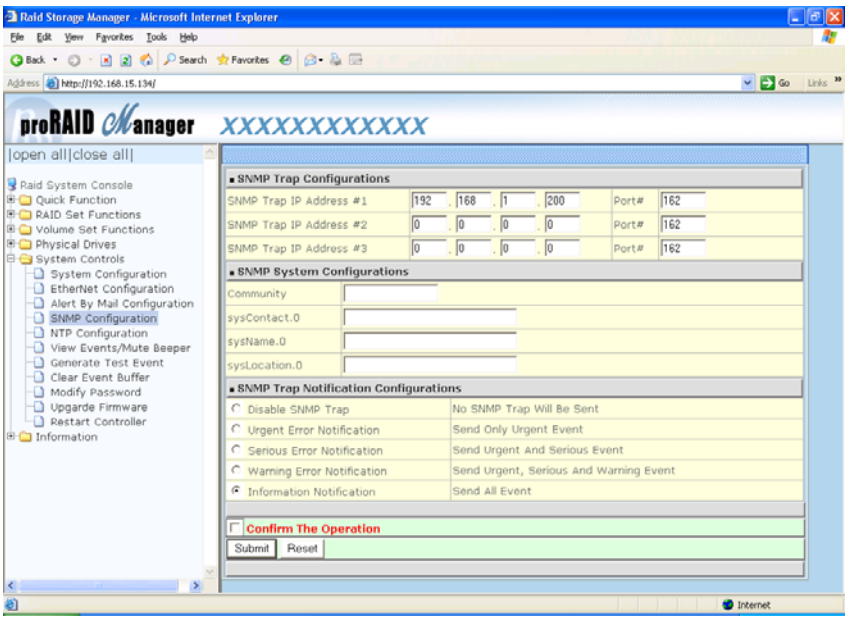


NOTE: If Event Notification by email is enabled, every 30 of event log will be sent to the email recipient(s) as one package log.

5.5.4 SNMP Configuration

The SNMP gives users independence from the proprietary network management schemes of some manufacturers and SNMP is supported by many WAN and LAN manufacturers enabling true LAN/ WAN management integration.

To set the SNMP function, move the cursor to the main menu and click on the **SNMP Configuration** link. The RAID subsystem's SNMP Configurations screen will be shown. Select the desired function and set the preferred option.



SNMP Trap Configurations: Type in the SNMP Trap IP Address box the IP address of the host system where SNMP traps will be sent. The SNMP Port is set to 162 by default.

SNMP System Configuration:

Community: Type the SNMP community. The default is public.
(1) **sysContact.0**, (2) **sysLocation.0**, and (3) **sysName.0**: SNMP parameter (31 bytes max). If these 3 categories are configured and when an event occurs, SNMP will send out a message that includes the 3 categories within the message. This allows user to easily define which RAID unit is having problem.

SNMP Trap Notification Configurations: Select the desired option.

After completing the settings, tick on the **Confirm The Operation** and click on the **Submit** button to save the configuration.

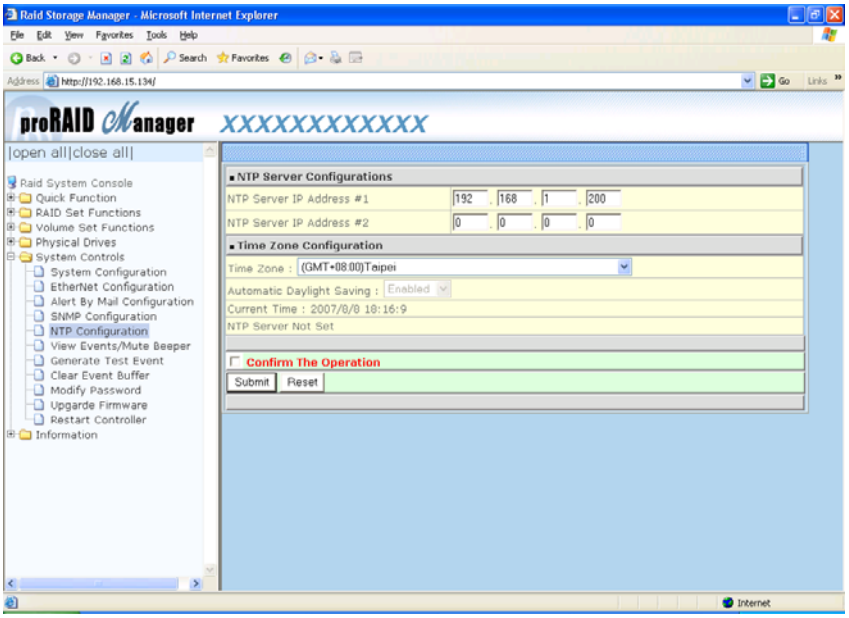
SNMP also works in the same as Alert By Mail when sending event notifications.

5.5.5 NTP Configuration

NTP stands for **Network Time Protocol**. It is an Internet protocol used to synchronize the clocks of computers to some time reference. Type the NTP Server IP Address to enable the RAID subsystem to synchronize with it.

To set the NTP function, move the cursor to the main menu and click on the **NTP Configuration** link. The RAID subsystem's NTP Configuration screen will be displayed. Select the desired function and configure the necessary option.

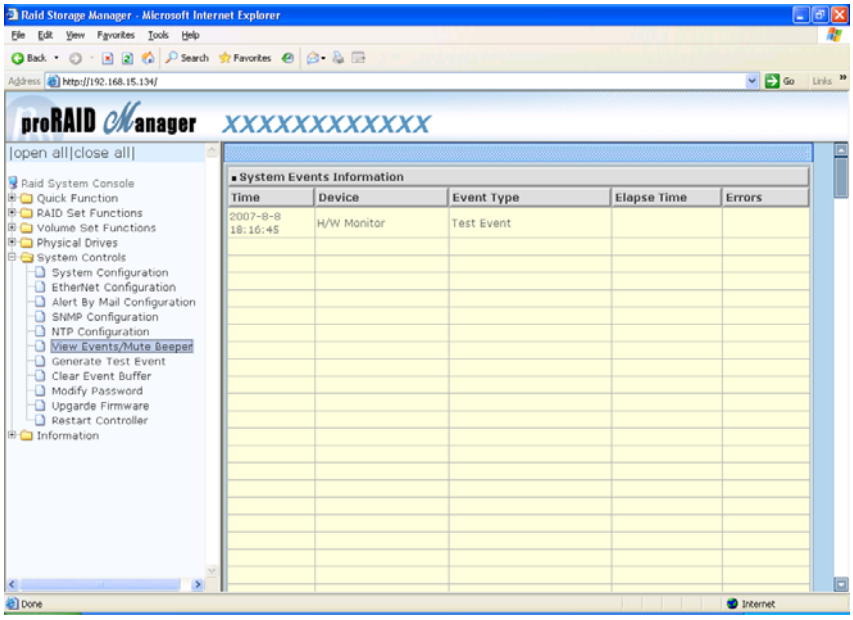
After completing the settings, tick on the **Confirm The Operation** and click on the **Submit** button to save the configuration.



5.5.6 View Events / Mute Beeper

To view the RAID subsystem's event log information, move the mouse cursor to the System Controls menu and click on the **View Events / Mute Beeper** link. The Raid Subsystem's System Events Information screen appears.

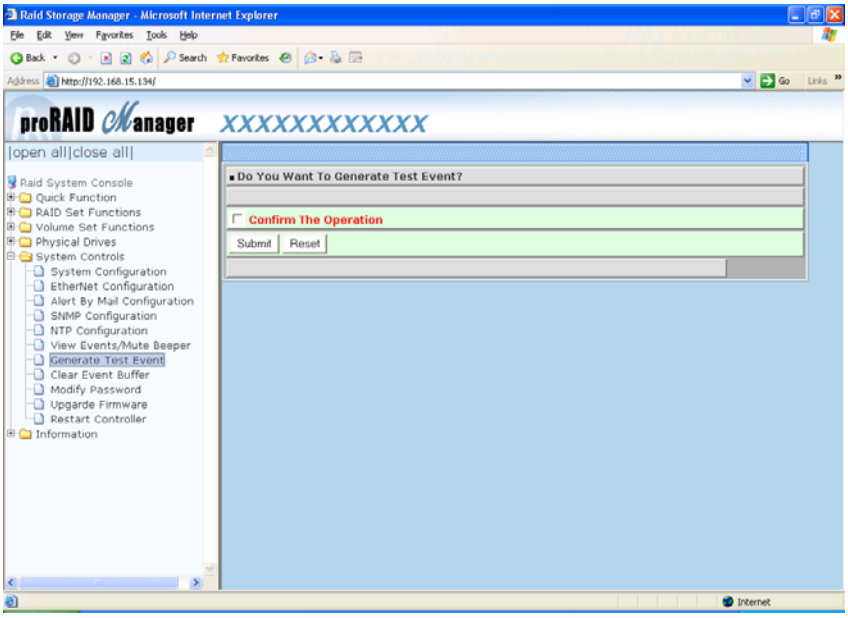
The System Events Information screen will show: Time, Device, Event type, Elapse Time and Errors.

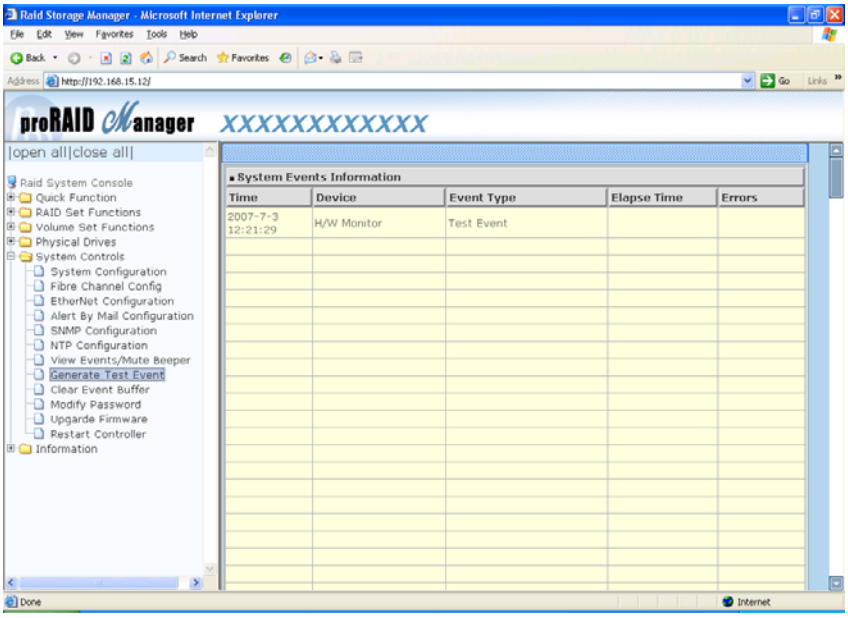


This function is also used to silence the beeper alarm.

5.5.7 Generate Test Event

If you want to generate test events, move the cursor bar to the main menu and click on the **Generate Test Event** Link. Tick on the **Confirm The Operation** and click on the **Submit** button. Then click on the **View Events/Mute Beeper** to view the test event.





5.5.8 Clear Event Buffer

Use this feature to clear the RAID subsystem's System Events Information buffer.

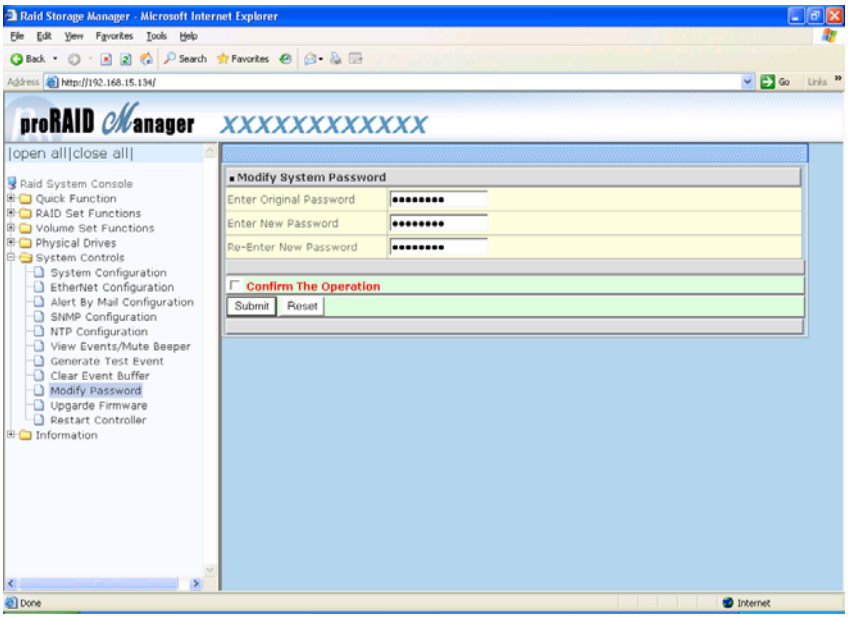
5.5.9 Modify Password

To change or disable the RAID subsystem's admin password, click on the **Modify Password** link under the **System Controls** menu. The Modify System Password screen appears.

The factory-default admin password is set to **00000000**. Once the password has been set, the user or administrator can only monitor and configure the RAID subsystem by providing the correct password.

The password is used to protect the RAID subsystem's configuration from unauthorized access. The RAID controller will check the password only when entering the Main Menu from the initial screen. The RAID subsystem will automatically go back to the initial screen when it does not receive any command after sometime.

To disable the password, enter only the original password in the **Enter Original Password** box, leave both the **Enter New Password** and **Re-Enter New Password** boxes blank. After selecting the **Confirm The Operation** option and clicking the **Submit** button, the system password checking will be disabled. No password checking will occur when entering the main menu from the starting screen.



5.5.10 Upgrade Firmware

Please refer to Section 6.2 for more information.

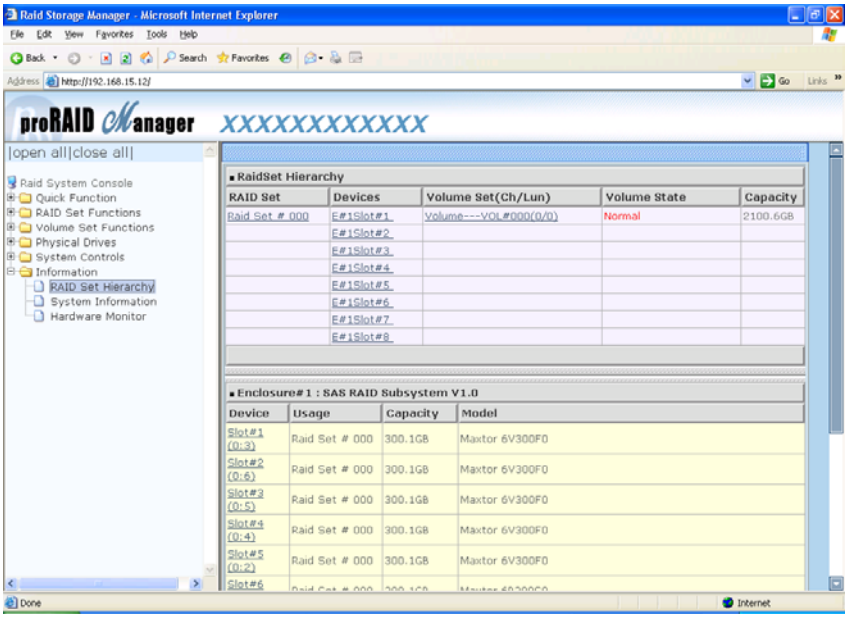
5.5.11 Restart Controller

Use this function to restart the RAID Controller.

5.6 Information Menu

5.6.1 RAID Set Hierarchy

Use this feature to view the RAID subsystem's existing Raid Set(s), Volume Set(s) and disk drive(s) configuration and information. Select the **RAID Set Hierarchy** link from the **Information** menu to display the Raid Set Hierarchy screen.



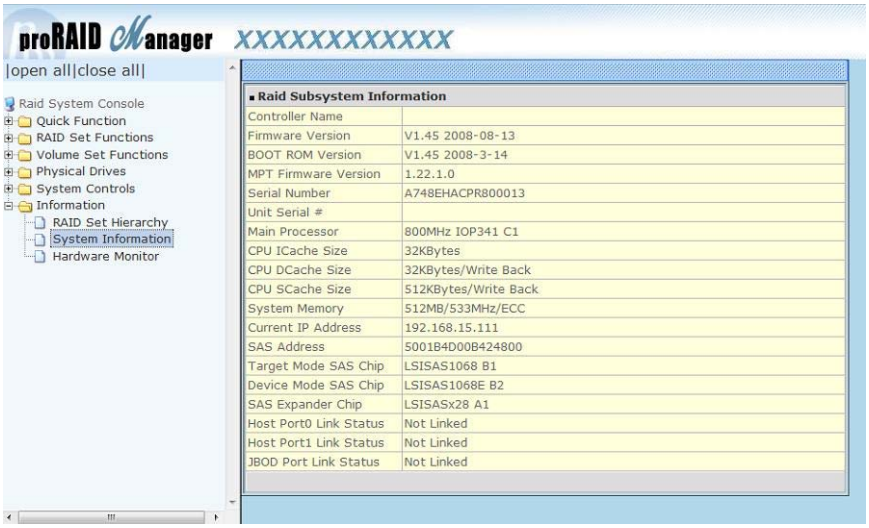
To view the Raid Set information, click the **Raid Set #** link from the Raid Set Hierarchy screen. The Raid Set Information screen appears.

To view the disk drive information, click the **Slot#** link from the Raid Set Hierarchy screen. The Disk Information screen appears. This screen shows various information such as timeout count, media error count, and SMART information.

To view the Volume Set information, click the **Volume---VOL#** link from the Raid Set Hierarchy screen. The Volume Set Information screen appears.

5.6.2 System Information

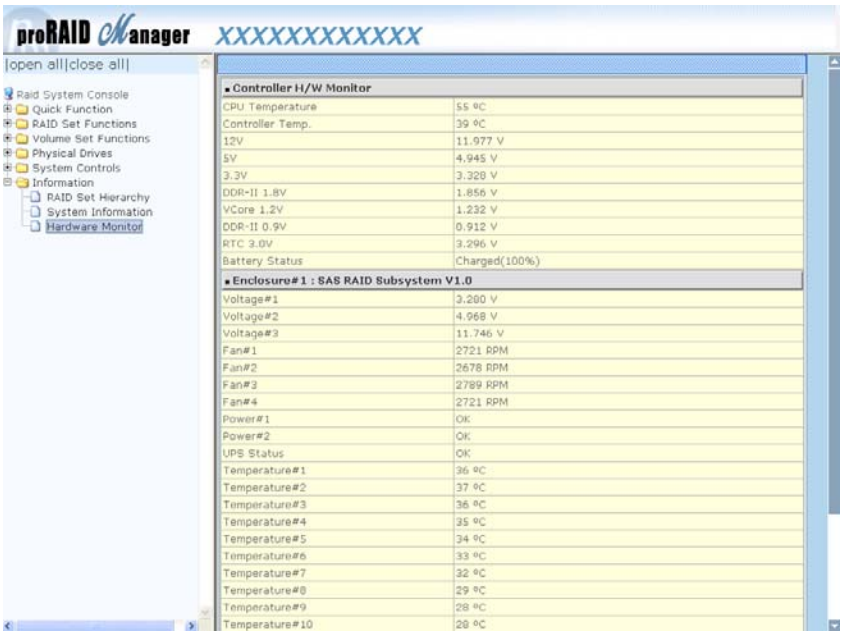
To view the RAID subsystem's controller information, click the **System Information** link from the **Information** menu. The Raid Subsystem Information screen appears.



The Controller Name, Firmware Version, Serial Number, Main Processor, CPU Data/Instruction Cache size, System Memory size/speed, Current IP Address, SAS Address, Target Mode SAS Chip, Device Mode SAS Chip, SAS Expander Chip, Host Port Link Status, and JBOD Port Link Status appear in this screen.

5.6.3 Hardware Monitor

To view the RAID subsystem's hardware information, click the **Hardware Monitor** link from the **Information** menu. The Hardware Monitor Information screen appears.



The Hardware Monitor Information provides the temperature, fan speed (chassis fan) and voltage levels of the RAID subsystem. All items are also unchangeable. When the threshold values are surpassed, warning messages will be indicated through the LCD, LED and alarm buzzer.

Item	Warning Condition
Controller Board Temperature	**> 70 Celsius**
HDD Temperature	**> 65 Celsius**
Controller Fan Speed	**< 1500 RPM**
Power Supply +12V	**< 10.5V or > 13.5V**
Power Supply +5V	**< 4.7V or > 5.4V**
Power Supply +3.3V	**< 3.0V or > 3.6V**
DDR Supply Voltage +2.5V	**< 2.25V or > 2.75V**
CPU Core Voltage +1.3V	**< 1.17V or > 1.43V**
DDR Termination Power +1.25V	**< 1.125V or > 1.375V**

Chapter 6 System Maintenance

RAID Subsystem

6.1 Upgrading the RAID Controller's Cache Memory

The RAID controller is equipped with one DDRII SDRAM socket. By default, the RAID controller comes with 512MB of memory that is expandable to a maximum of 4GB. The expansion memory module can be purchased from your dealer.

Memory Type: 1.8V PC5300/4200 DDR2 SDRAM 240pin ECC.
Memory Size: Supports 240pin DDRII of 512MB, 1GB, 2GB, or 4GB.

6.1.1 Installing Memory Module

1. Shutdown first the NAS system and unplug all power cords.
2. Press the push button lock on the top cover, and pull the top cover handle towards the rear. Then remove the top cover.
3. Remove the memory module from the RAM socket of the RAID controller by pressing the ejector clips until the memory module pops out of the socket.
4. Align the new memory module into the socket. Make sure the notch is aligned with the key on the socket itself. With the ejector clips in open position, press down the memory module into the socket until it sinks into place. The ejector clips will automatically close to lock the memory module.

6.2 Upgrading the RAID Controller's Firmware

Upgrading Firmware Using Flash Programming Utility

Since the RAID subsystem's controller features flash firmware, it is not necessary to change the hardware flash chip in order to upgrade the controller firmware. User can simply re-program the old firmware through the RS-232 port. New releases of the firmware are available in the form of binary file at vendor's FTP. The file available at the FTP site is usually a self-extracting file that contains the following:

XXXXVVV.BIN Firmware Binary (where "XXXX" refers to the model name and "VVV" refers to the firmware version)

README.TXT It contains the history information of the firmware change. Read this file first before upgrading the firmware.

These files must be extracted from the compressed file and copied to one directory in the host computer.

Establishing the Connection for the RS-232

The firmware can be downloaded to the RAID subsystem's controller using an ANSI/VT-100 compatible terminal emulation program or web browser-based RAID Manager remote management page.

With terminal emulation program, you must complete the appropriate installation and configuration procedure before proceeding with the firmware upgrade. Whichever terminal emulation program is used must support the ZMODEM file transfer protocol.

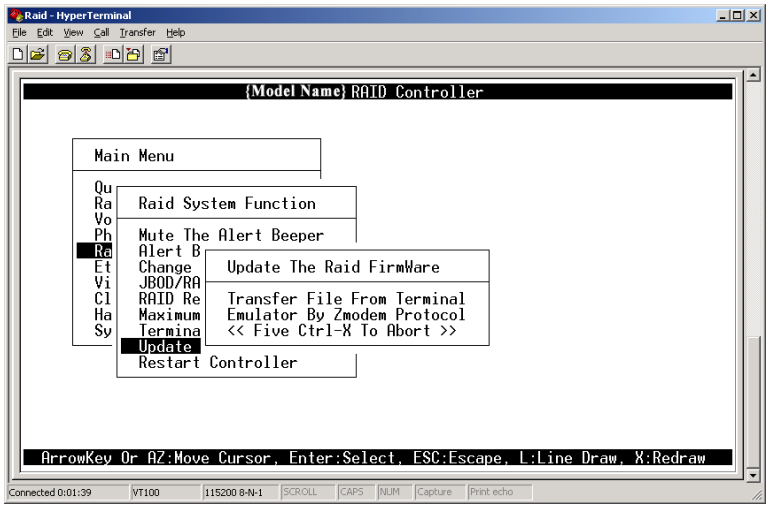
Web browser-based RAID Manager can be used to update the firmware. A web browser must have been setup before proceeding with the firmware upgrade.

Upgrading Firmware Through ANSI / VT-100 Terminal Emulation

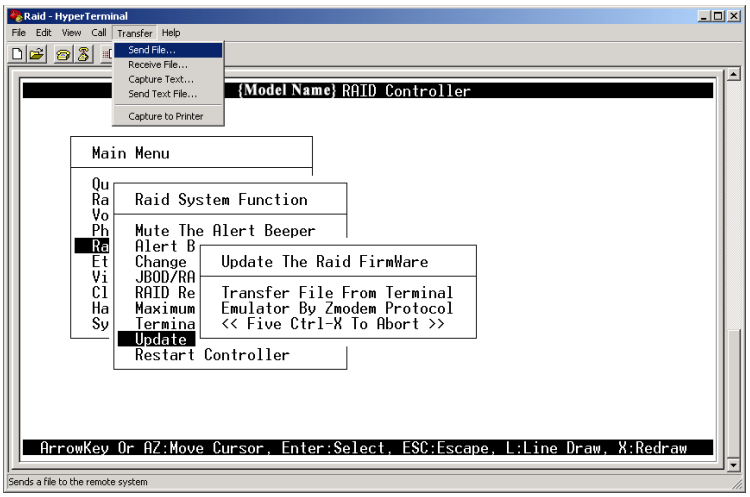
Get the new version firmware for your RAID subsystem controller. For Example, download the bin file from your vendor's web site into the local directory.

NOTE: When there is new boot ROM firmware that needs to be upgraded, upgrade first the boot ROM firmware. Then repeat the process (steps 1 to 9) to upgrade the firmware code after which a RAID controller restart will be necessary.

1. From the Main Menu, scroll down to "Raid System Function"
2. Choose the "Update Firmware". The **Update The Raid Firmware** dialog box appears.

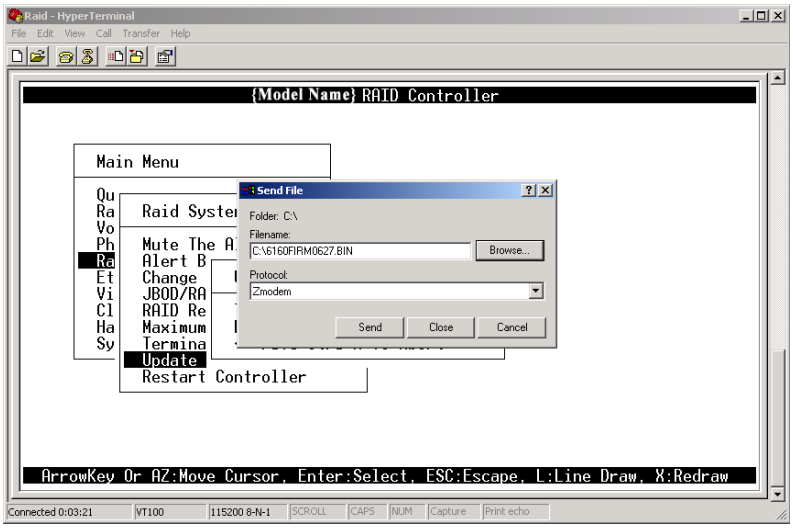


3. Go to the menu bar and click **Transfer**. Select **Send File**.

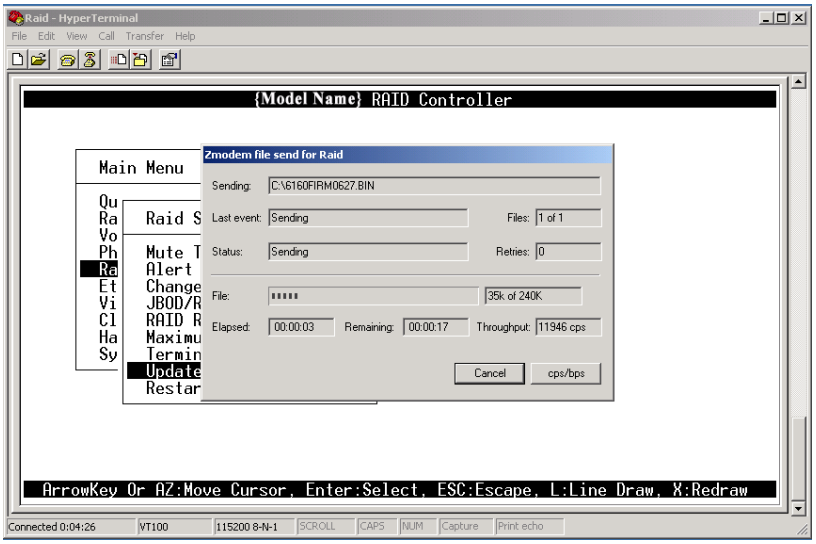


4. Select "ZMODEM modem" under Protocol to set ZMODEM as the file transfer protocol of your terminal emulation software.

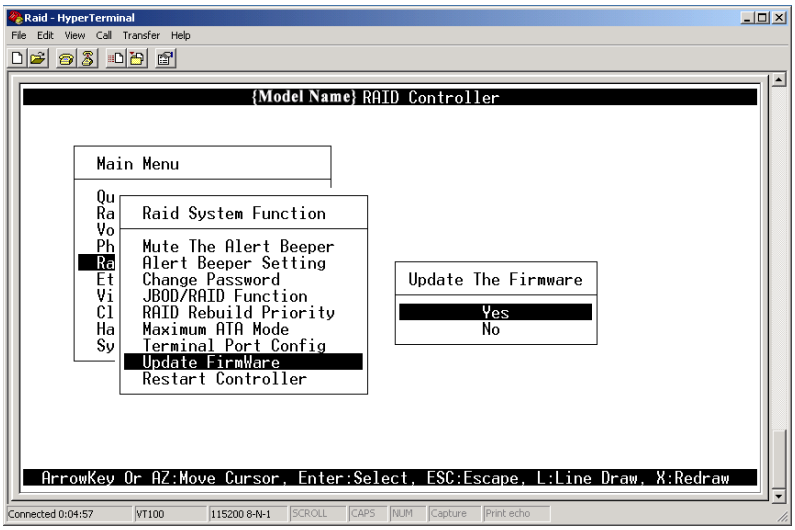
5. Click Browse. Look in the location where the firmware file was saved. Select the firmware file name “XXXXXXXX.BIN” and click Open.



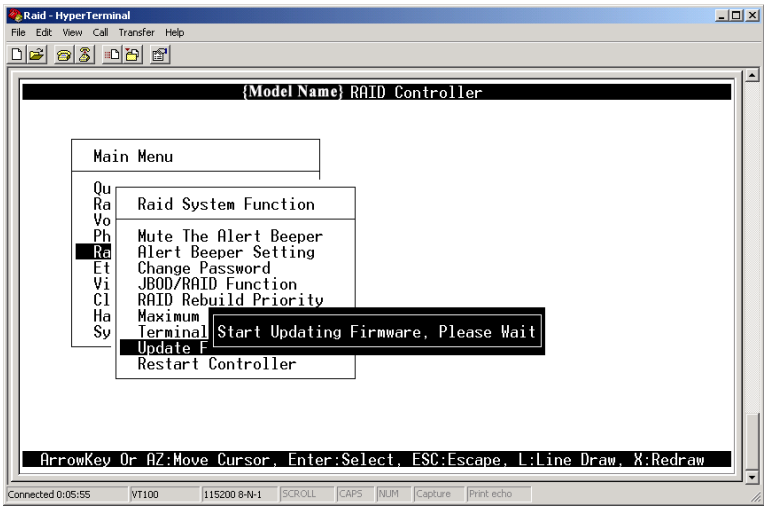
6. Click Send to send the firmware binary file to the RAID controller.



7. When the firmware downloading is completed, the confirmation screen appears. Select Yes to start programming the flash ROM.

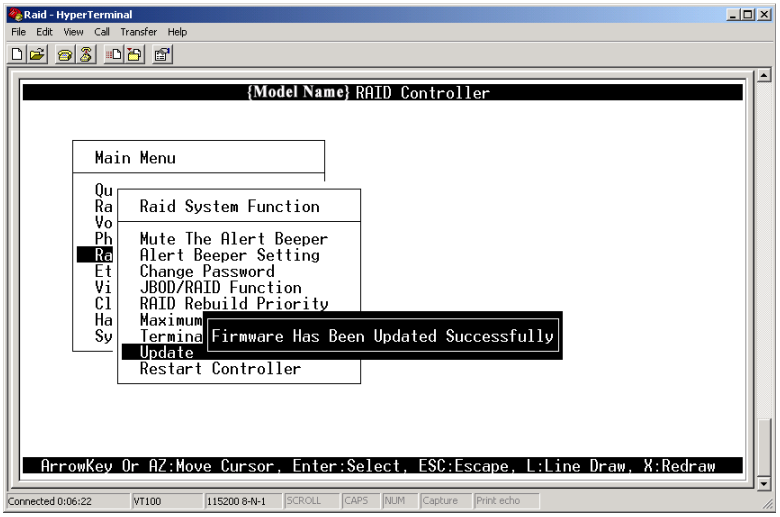


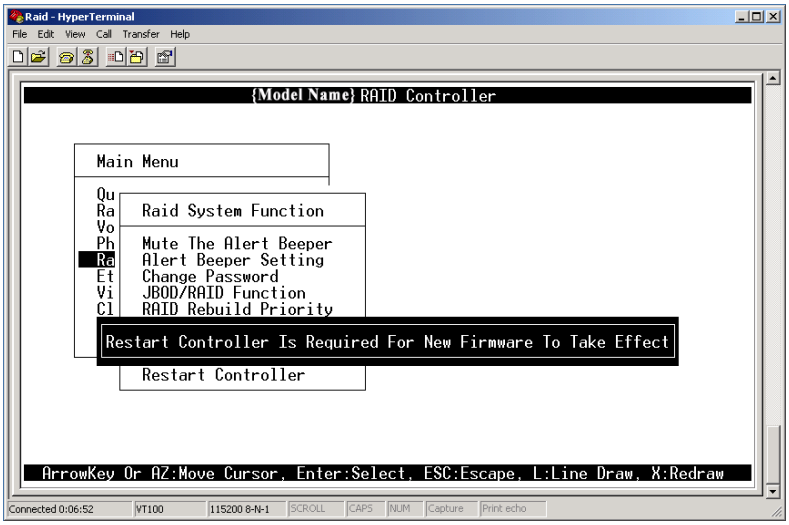
8. When the Flash programming starts, a message will show “Start Updating Firmware. Please Wait”.



9. The firmware upgrade will take approximately thirty seconds to complete.

10. After the firmware upgrade is complete, a message will show “Firmware Has Been Updated Successfully”. Restarting the RAID controller is required for the new firmware to take effect.



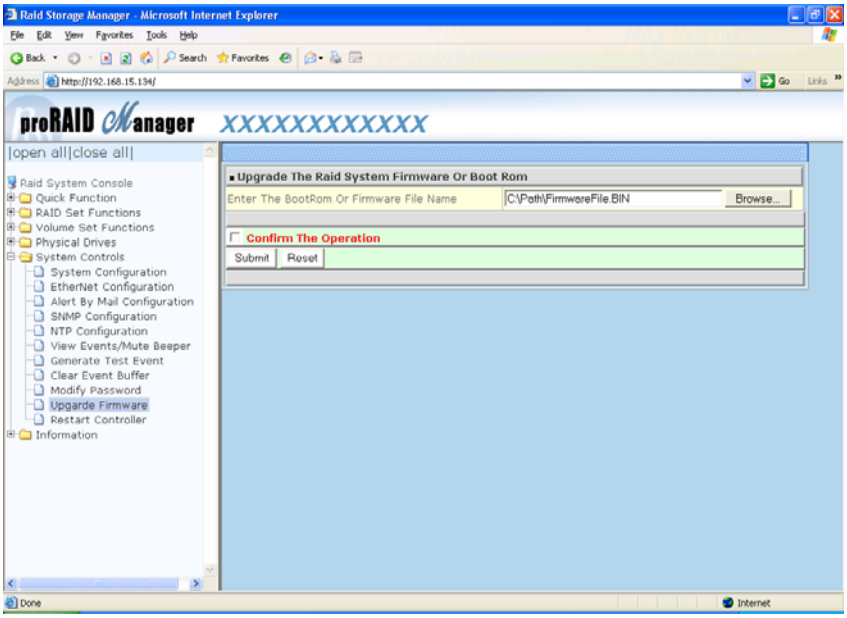


Upgrading Firmware Through Web Browser

Get the new version of firmware for your RAID subsystem controller.

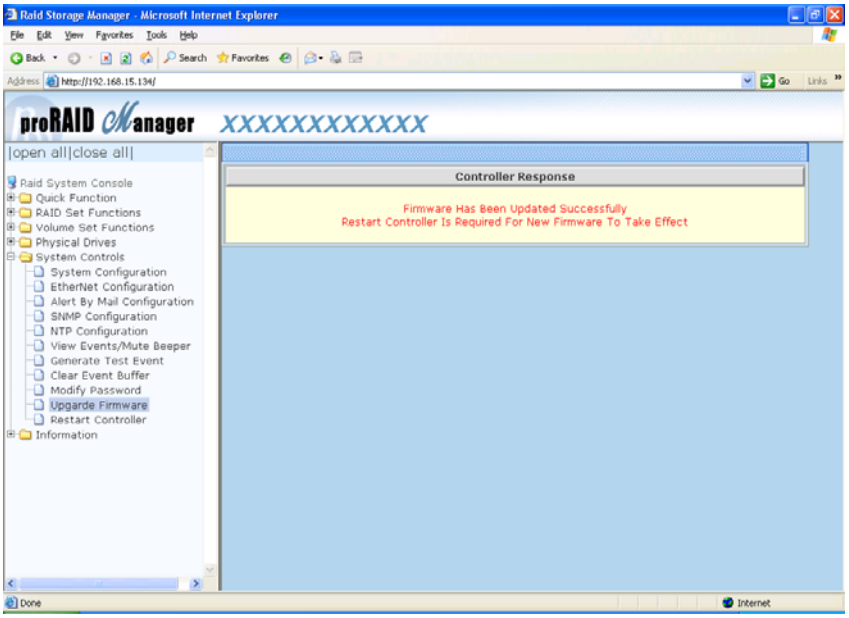
NOTE: When there is new boot ROM firmware that needs to be upgraded, upgrade first the boot ROM firmware. Then repeat the process (steps 1 to 3) to upgrade the firmware code after which a RAID controller restart will be necessary.

1. To upgrade the RAID subsystem firmware, click the **Upgrade Firmware** link under **System Controls** menu. The Upgrade The Raid System Firmware Or Boot Rom screen appears.
2. Click **Browse**. Look in the location where the firmware file was saved. Select the firmware file name “XXXXXXXX.BIN” and click Open.
3. Select the **Confirm The Operation** option. Click the **Submit** button.



4. The Web Browser begins to download the firmware binary to the controller and start to update the flash ROM.

5. After the firmware upgrade is complete, a message will show “Firmware Has Been Updated Successfully”. Restarting the RAID controller is required for the new firmware to take effect.



PART II proNAS System

Chapter 7 Introduction

The NAS system comes with “proNAS” NAS management solution and “proBackup” client backup solution as well as proNAS HA solution (optional) to provide the enterprises the most flexible, scalable, securable and manageable NAS environment. Administrator can centralize and easily manage the NAS nodes via Internet/Intranet and enhance greater data availability via proNAS.

7.1 proNAS Key Components

- **NAS Device Manager**: Provides configuration of physical hard disks with hardware RAID Controller.

NOTE: This NAS model does not support NAS Device Manager. Use the web browser-based proRAID Manager GUI to configure the RAID controller.

- **proNAS Manager**: Provides several management tools to ease the NAS administration job.
  - Volume Manager: Responsible for volume management. Configuration of volume groups, logical volumes, volume snapshot and volume replication.
  - Account Manager: Local and external account configuration. Import large accounts.
  - Backup Manager: Supports system configuration backup and setup the backup plan for data backup.
  - Share Manager: Share configuration and ACL setting. This also includes Rsync and Duplication functions.
  - System Manager: System configuration and firmware upgrade
  - Network Manager: Configuration of network information and trunking.
  - Log Manager: Contains NAS system logs.
  - Event Manager: Configuration of email notification and system actions when events occur.

- **File Manager**: Provides user logon mode for share owner to perform folder and file management such as share folder access control.
- **proNAS HA**: (optional). Provides function of High Availability (two-node cluster) in Active-Standby mode.
- **proBackup**: Provides web-based GUI backup solution for desktop clients.

Each function of these components is described in the following Chapters.

NOTE: Some pictures and screenshots might be different from the actual NAS machine.

7.2 Installation and Configuration Phases

The installation and configuration of a proNAS system can be divided into five phases.

Phase 1: Set up the Hardware RAID Controller and create Raid Set and Volume Set.

Prior to proNAS system configuration, a basic hardware RAID configuration must be setup. Please refer to Section 7.3 for the basic setup instructions in creating Raid Set and Volume Set using proRAID Manager. For more information about Raid Set and Volume Set, refer to Chapter 5 Section 5.2 and 5.3.

Phase 2: Configure proNAS and its components with proNAS Manager. This is described in details in Chapter 8 proNAS Manager. To configure proNAS, you need to:

- Join a disk (Volume Set created in proRAID Manager) to the system default volume group "proNASVG" using Volume Manager. This is described in Chapter 8 Section 8.1.1 and 8.1.2.
- Configure the network settings via Network Manager. This is described in Chapter 8 Section 8.2.1.
- Create or import accounts with Account Manager as described in Chapter 8 Section 8.3.
- Setup the shares using Share Manager and assign account/group permissions. This is described in Chapter 8 Section 8.4.
- Windows clients can start using the proNAS shares using CIFS protocol. UNIX/Linux clients need to enable NFS protocol (disabled by default).

Phase 3: Perform NAS system maintenance.

- Maintain system via System Manager, as described in Chapter 8 Section 8.5
- Check system status using Log Manager and Event Manager. This is described in Chapter 8 Sections 8.7 and 8.8.
- Backup system configuration and data using Backup Manager. This is described in Chapter 8 Section 8.6.

Phase 4: (Optional) Setup proNAS HA for high-availability environment. Please refer to Chapter 11 for proNAS HA configuration.

Phase 5: Users can store and backup data into proNAS system.

- Store data into proNAS system using File Manager, as described in Chapter 9.
- Backup data into proNAS system using proBackup, as described in Chapter 10.

7.3 Basic Setup Instructions in Creating Raid Set and Volume Set

NOTE: If you already created a Raid Set and Volume Set, you may skip this section.

This example creates a single Raid Set using 16 disk drives and a single Volume Set RAID Level 5 with over 2TB capacity.

1. To login to proRAID Manager GUI:

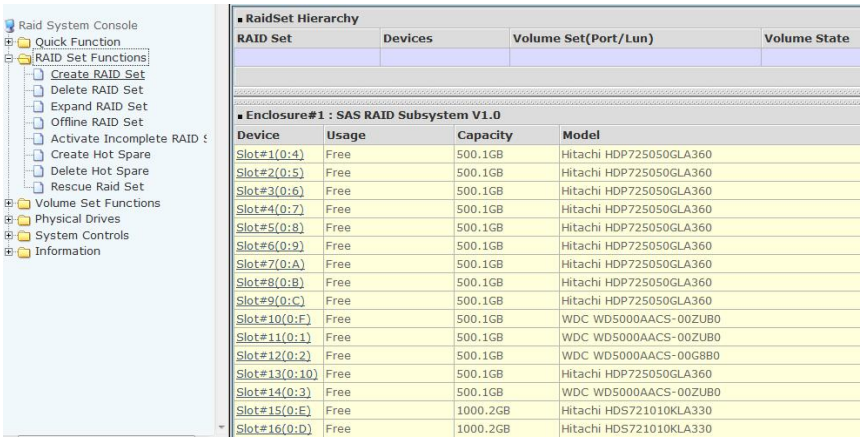
   a. Reconfigure the network settings of your client computer to be able to connect to R-Link IP address 172.16.0.2 (displayed in LCD panel), if not yet configured.

   b. Open web browser and type http://xxx.xxx.xxx.xxx in the address bar (where xxx.xxx.xxx.xxx is the R-Link IP address. Default R-Link IP address is 172.16.0.2, subnet mask 255.255.0.0).

   c. To login to proRAID Manager GUI, enter user name “admin” and default password “00000000” (8 zeroes).

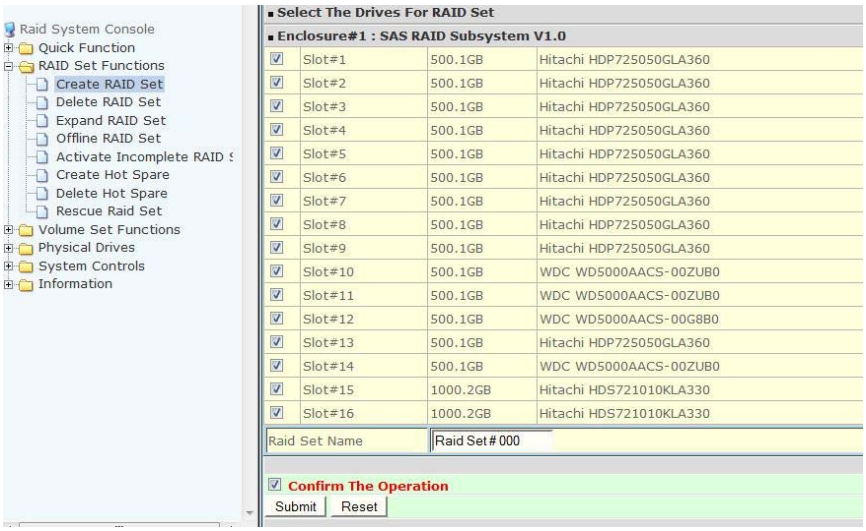
2. Create Raid Set

   a. Click **RAID Set Functions** to expand the menu.



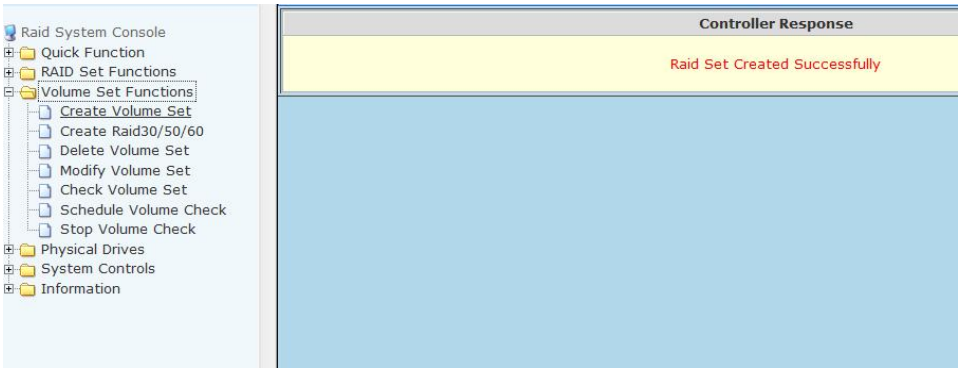
   b. Click **Create RAID Set** link.

c. Select the disk drives to be included in the RAID Set. Tick “Confirm The Operation” and click “Submit” button. The RAID Set will be created.



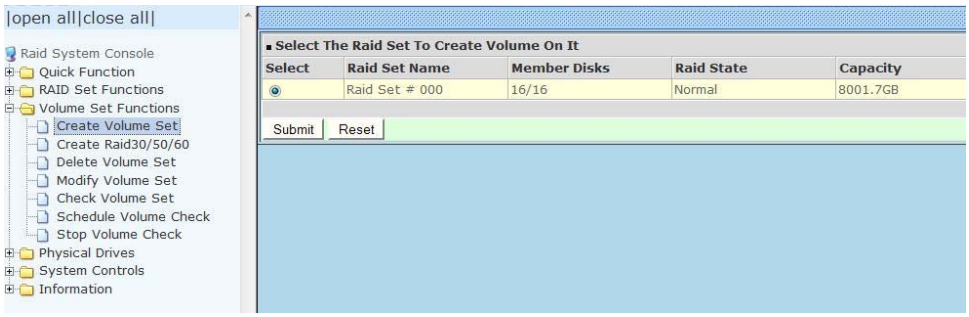
3. Create Volume Set

a. Click **Volume Set Functions** to expand the menu.

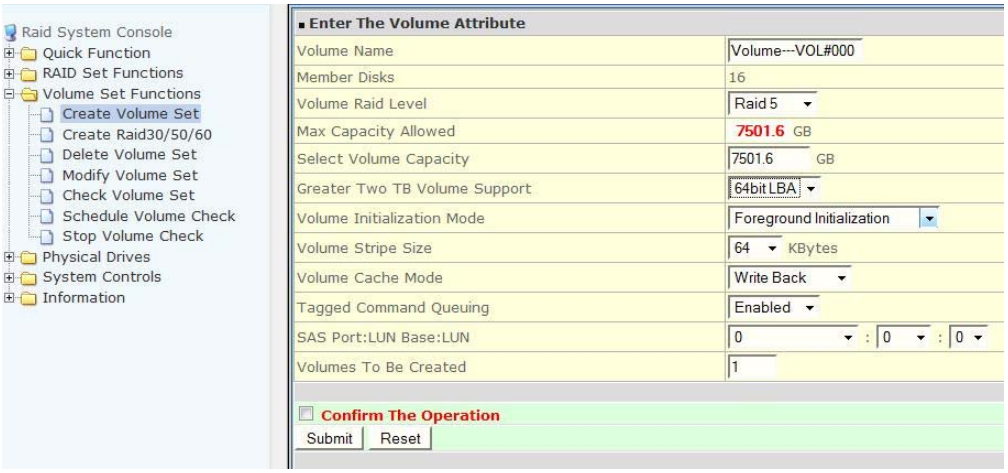


b. Click **Create Volume Set** link.

c. The Raid Set Name which you created before is automatically selected. Click “Submit” button.



d. Configure the Volume Raid Level you want. To create a single Volume Set with over 2TB capacity, select “64bit LBA” in Greater Two TB Volume Support.



e. Tick “Confirm The Operation” and click on “Submit” button. The Volume Set will be created and initialize in Foreground mode. When the Volume Set initialization is completed, reboot the NAS system.

7.4 Setting proNAS IP Address and Connecting to NAS Management GUI

NOTE: Java 2 Runtime Environment (J2RE) 1.4.2 or later must be installed before using the proNAS management interface. (Free download from: http://java.sun.com/j2se/index.jsp)

1. If necessary, reconfigure the network settings of your client computer to be able to connect to LAN0 IP address 172.16.0.1 (see table below), or add IP address 172.16.0.5 subnet 255.255.0.0.

Entity	Default Value
LAN0 IP address	172.16.0.1
Subnet Mask	255.255.0.0
Hostname	proNAS
Username	admin
Password	proware

NAS Default Values

2. To connect to NAS administration page, open Web browser.
3. Enter the following URL in the address bar: http://172.16.0.1 then press Enter.
4. In the page that opens, click “Admin Login” command button to enter the NAS administration page.

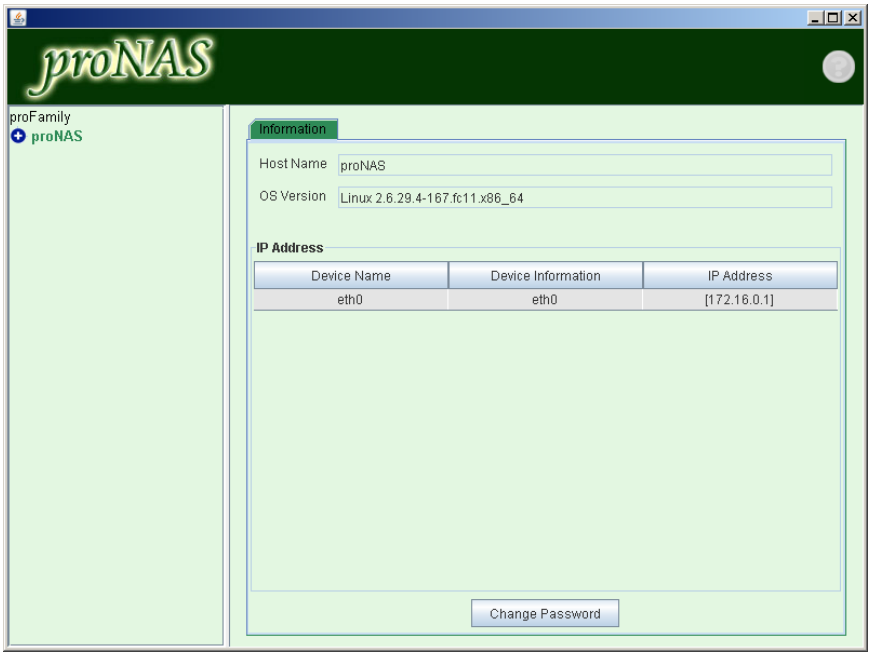
START button on the first proNAS

5. Enter Account as “admin” and password as “proware” and click the Logon command button.

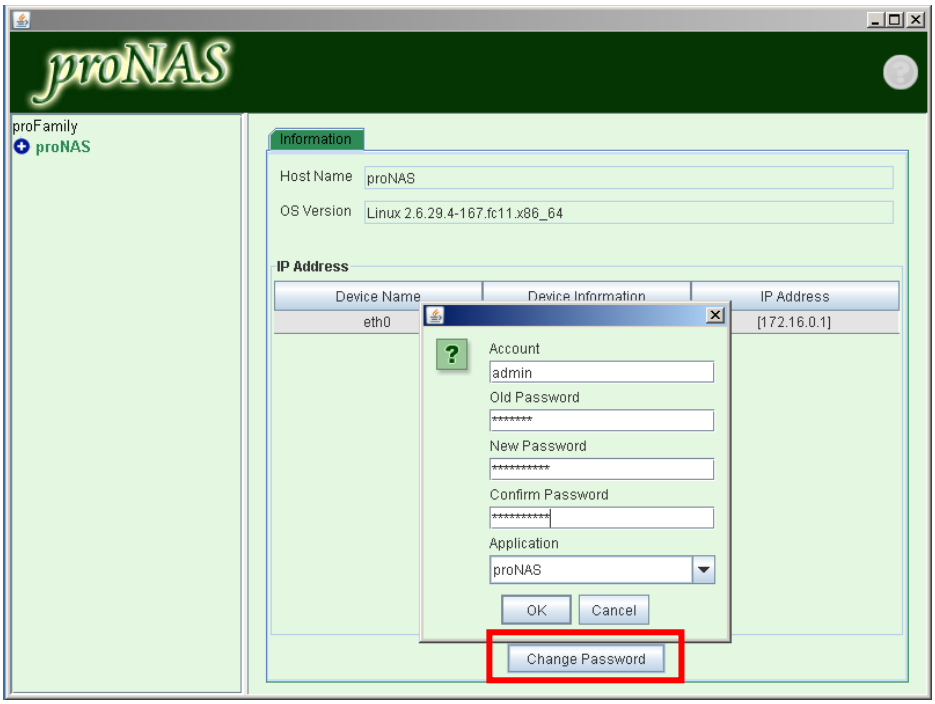
Login Screen

NOTE: proNAS supports language options: English, Chinese (Taiwan), Chinese (China), Japanese, Korean, German (Germany), Polish (Poland), and Russian (Russia). You can select your preferred language before logon.

6. The proNAS Manager main screen will be displayed showing proNAS, NAS Device Manager, and Event Manager.



NOTE: For security reason, it is necessary to change the default admin password. To change admin password, click the "Change Password" button and enter the new password.

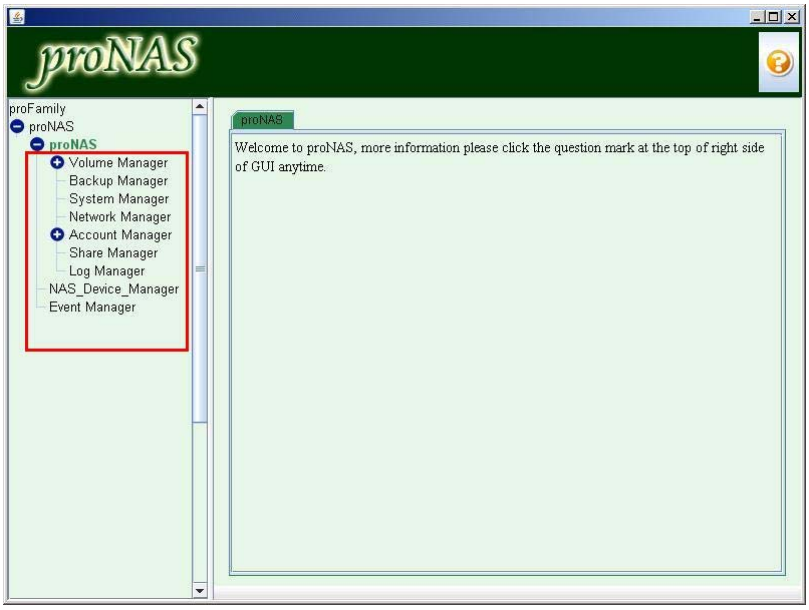


Chapter 8 proNAS Manager

proNAS supports Multi-Node Management. If you have several NAS subsystems connected to the intranet, you can see all these systems when you login to the proNAS system. The IP Address section lists the NAS systems connected to the network. proNAS Multi-Node Technology is based on UDP Multi-Casting technology. The proNAS managers are listed below.

The proNAS managers are:

1. Volume Manager
2. Network Manager
3. Account Manager
4. Share Manager
5. System Manager
6. Backup Manager
7. Log Manager
8. Event Manager



8.1 Volume Manager

The Volume Manager is responsible for disk and volume management.

A Volume Group consists of one or more disks that could be individual physical disk(s) or RAID disk(s), which is/are Volume(s) created using proRAID Manager. The default proNAS Volume Group (proNASVG) must be created first by joining at least one “New” or “Non_Initialized” disk to this volume group. The proNASVG holds the NAS system configuration and the default system Logical Volumes, such as home, public, proBackup Device, and proBackup Extended Device, as well as user-defined Logical Volumes. Files and folders reside on these Logical Volumes.

The default proNASVG Volume Group cannot be deleted. When proNASVG is created, the XFS file system is set in each default Logical Volume. XFS file system is also set in all user-defined Logical Volumes. XFS is a high performance journaling file system and provides better recovery time to repair a file system in case of FS damage. The proNAS Volume Group will dynamically allocate some space from its assigned disks, and allocation may fail if no more disk space is available. Therefore, make sure to regularly monitor the available free space of proNAS Volume Group.

The Volume Manager can perform the following function:

- Create a VG (volume group)
- Join New Disks
- Reset a VG (volume group)
- Remove a VG (volume group)
- Create Logical Volume
- Create Snapshot
- Create Replication
- Create iSCSI Target LUN

8.1.1 Volume Group Management

Volume Group (VG) is created by joining at least one disk, which can be physical disk or RAID disk(s). Logical Volumes are created under the Volume Group.

proNASVG is the system default VG. It must be created first in order to use the NAS system. To create the proNASVG, it is necessary to join at least one “New” or “Non_Initialized” disk into proNASVG.

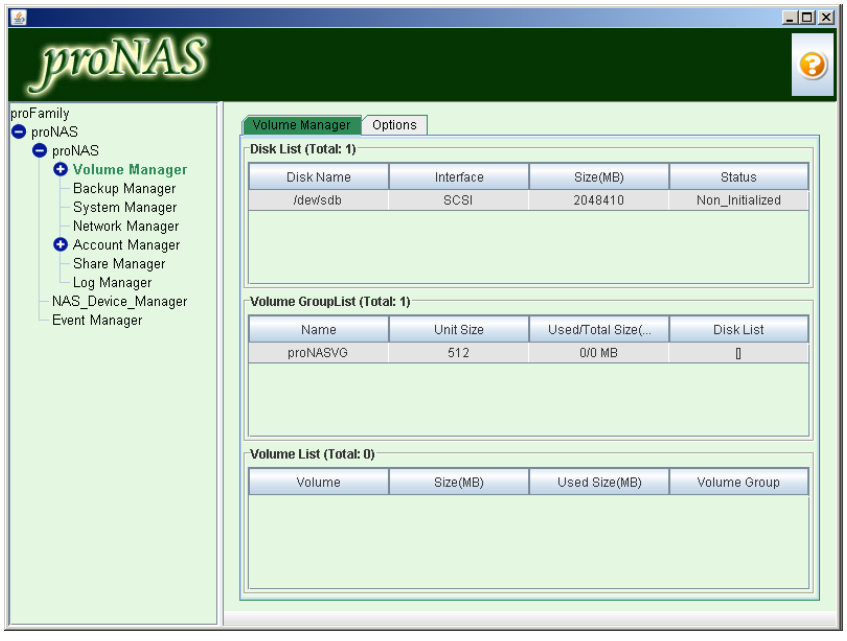
Admin can create other VG by joining other new or “Non_Initialized” disk, create or remove LV in this VG, join any new disk, remove any disk and reset the VG.

NOTE: If the Disk List in Volume Manager does not show any RAID disk (for example: /dev/sda) but a Raid Set and Volume Set has been created already, it is necessary to restart the proNAS system. Go to System Manager, select Reboot tab, and click Reboot Now button. Then re-login to NAS administration page.

8.1.1.1 Create the proNASVG Volume Group

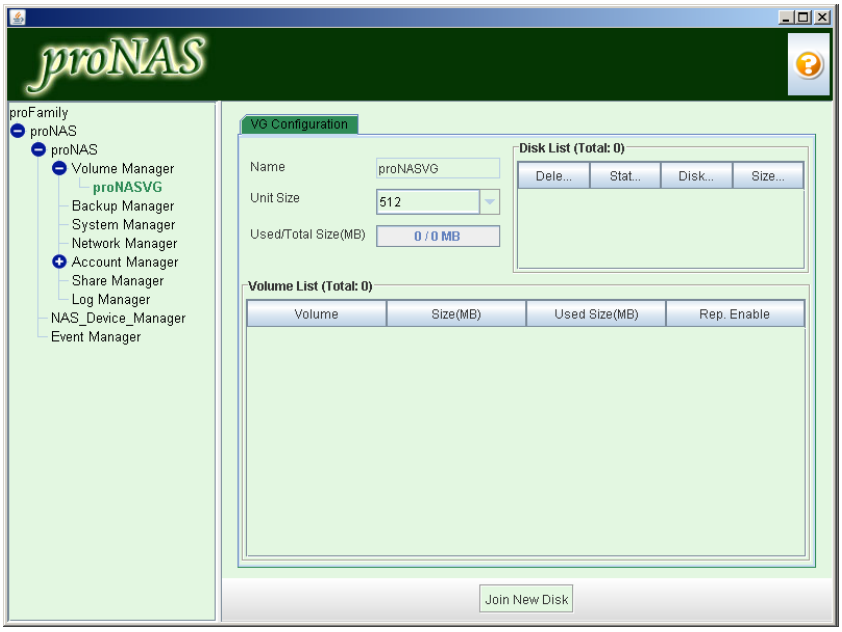
To create the proNASVG, perform the following steps:

1. In the proFamily tree, select Volume Manager. Verify that the Disk List shows at least one disk and the Status is “Non_Initialized’. Noticed in the Volume Group List that the proNASVG has no Disk List.



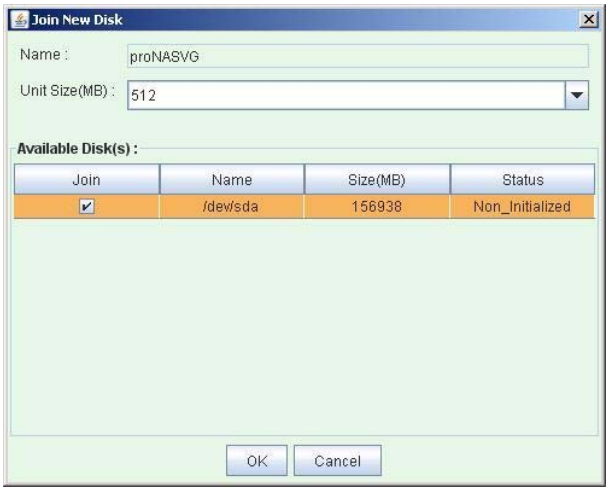
NOTE: The system default Volume Group “proNASVG” cannot be deleted or reset.

2. Select proNASVG under Volume Manager and click “Join New Disk” button.

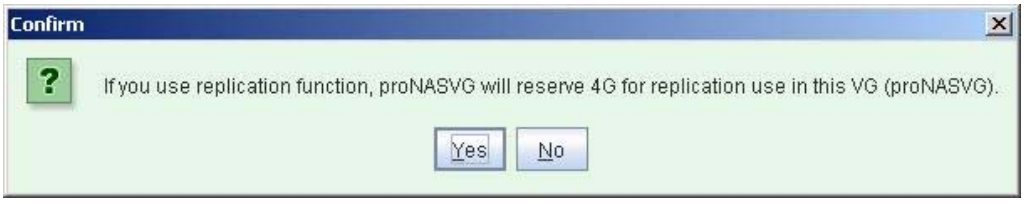


3. Select the Disk(s) that will be joined to proNASVG from the list of Available Disk(s). Click “OK” when done.

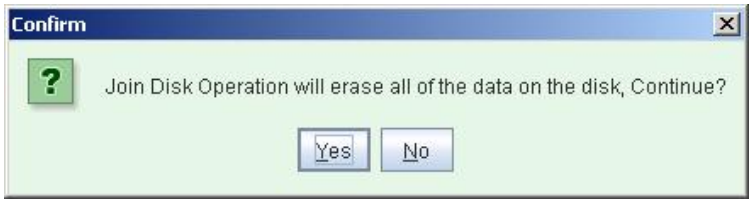
NOTE: Unit Size is the Physical Extent or block size used in the Volume Group. The VG Unit Size is set to 512MB and cannot be changed.



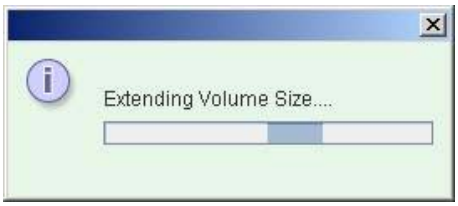
4. A confirmation message will appear. Select “Yes” to proceed.



5. Another confirmation message will appear. Select “”Yes” to proceed.

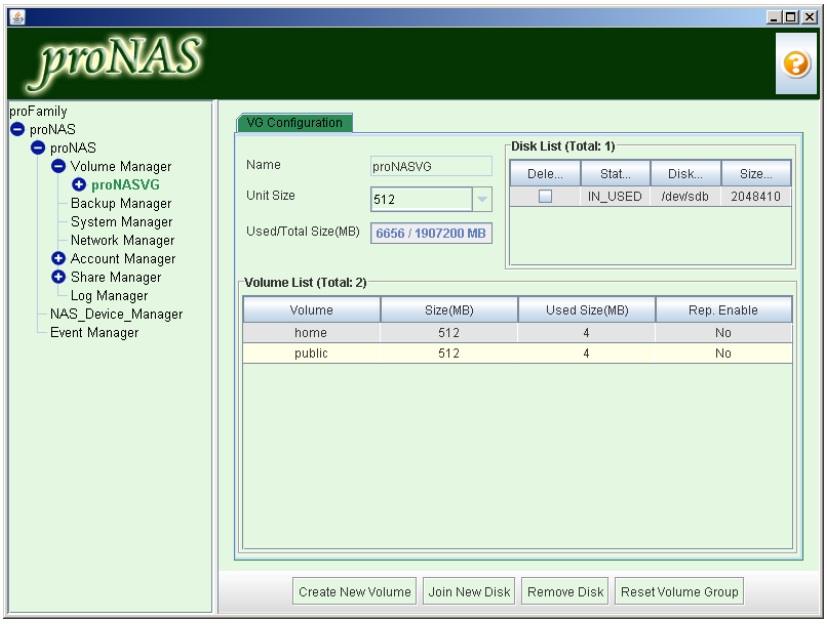


6. The process of joining disk to the VG will start.



7. When the process of joining disk to VG is completed, the NAS will reboot to free some used system memory. A warning message will be displayed. Click “OK” to close the message.

8. Wait for about 3 minutes then re-login to proNAS management GUI. The Volume Manager will show the joined disk as “IN_USED” and the Volume List will show the system default Logical Volumes “home” and “public”.



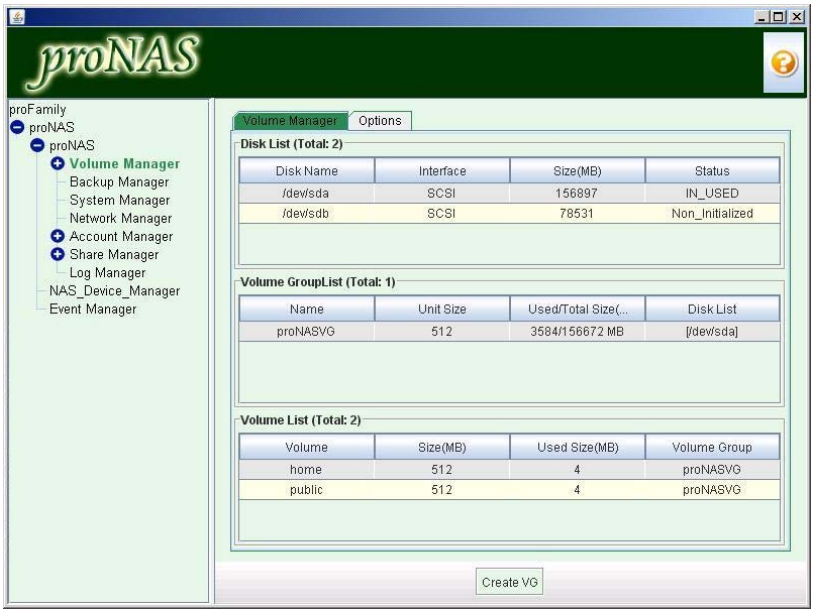
NOTE: The other system default LVs proBackup Device and proBackup Extended Device will only be created and become visible in the Volume List when the proBackup Service is started.

8.1.1.2 Creating another Volume Group

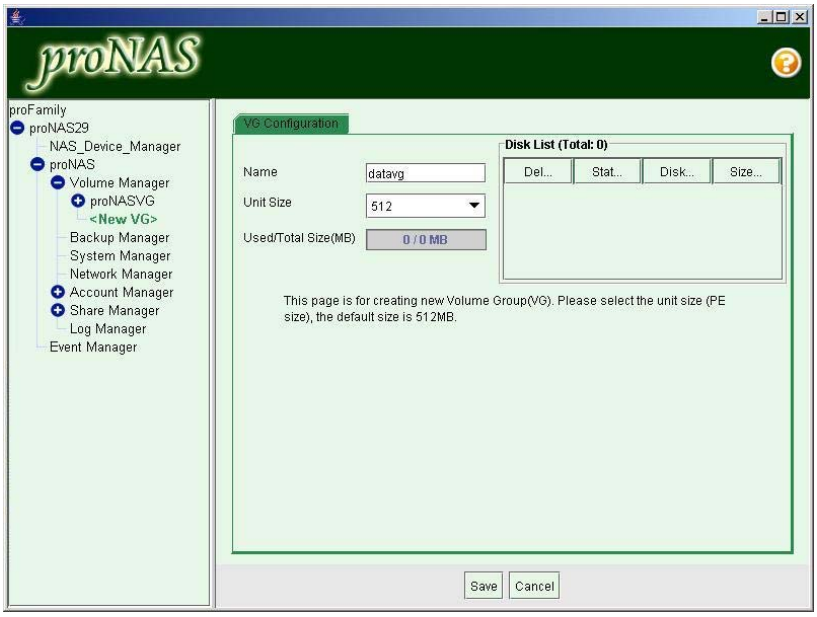
To create another VG, verify from Volume Manager Disk List if there is available free or "Non_Initialized" disk. If there is none, a new Volume Set (RAID disk) must be created first using proRAID Manager. If a new Volume Set has already been created, the NAS system must be restarted in order to detect the new RAID disk. To restart the NAS, select System Manager under proNAS, then click Reboot tab then click "Reboot Now" button. Re-login to NAS administration page after reboot.

To create another VG, perform the following steps:

1. In Volume Manager, click "Create VG" button.

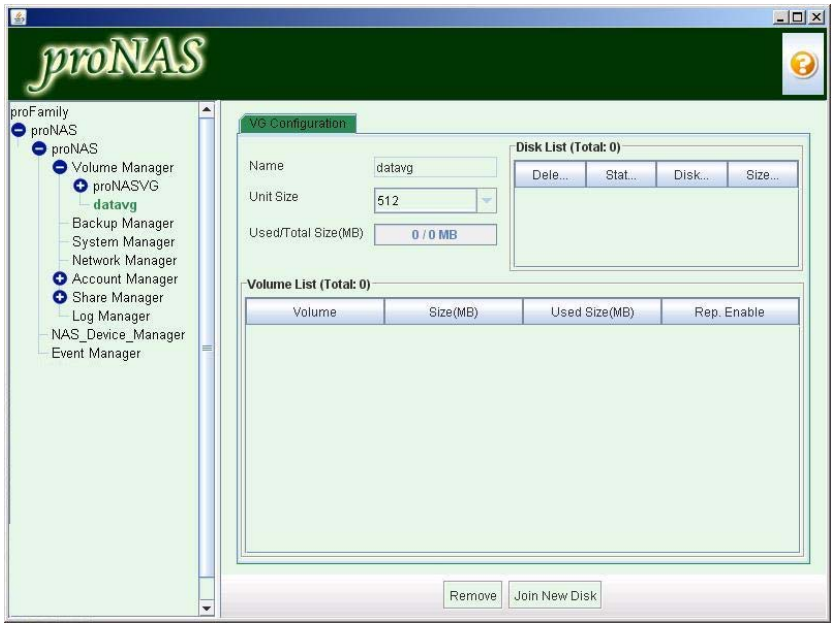


2. Enter the Volume Group Name. Click "Save" when done.

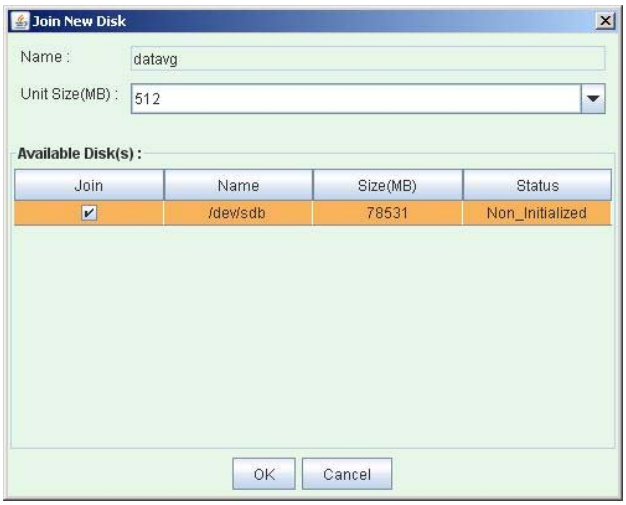


3. A confirmation message will appear. Select “Yes” to proceed.

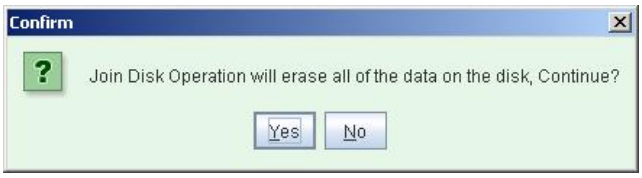
4. Click “Join New Disk” to continue with creating the new Volume Group.



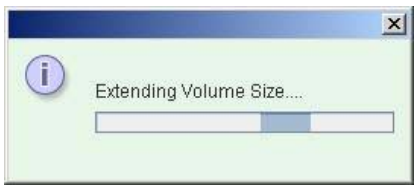
5. Check the disk(s) to be joined to the VG. Click “OK” when done.



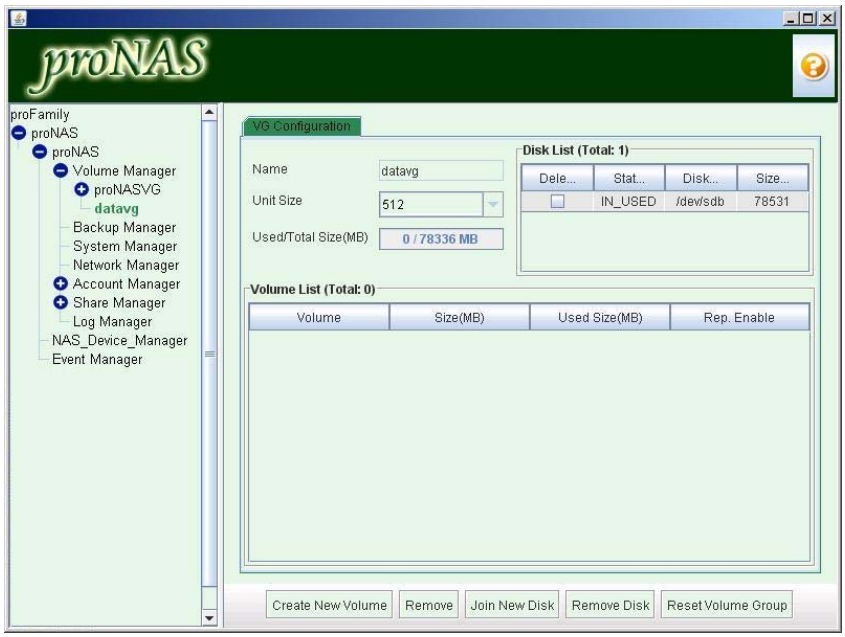
6. A confirmation message will appear. Select “Yes” to proceed.



7. A process window will appear.



8. When the process of joining disk to the new VG is completed, the newly created VG will be shown.



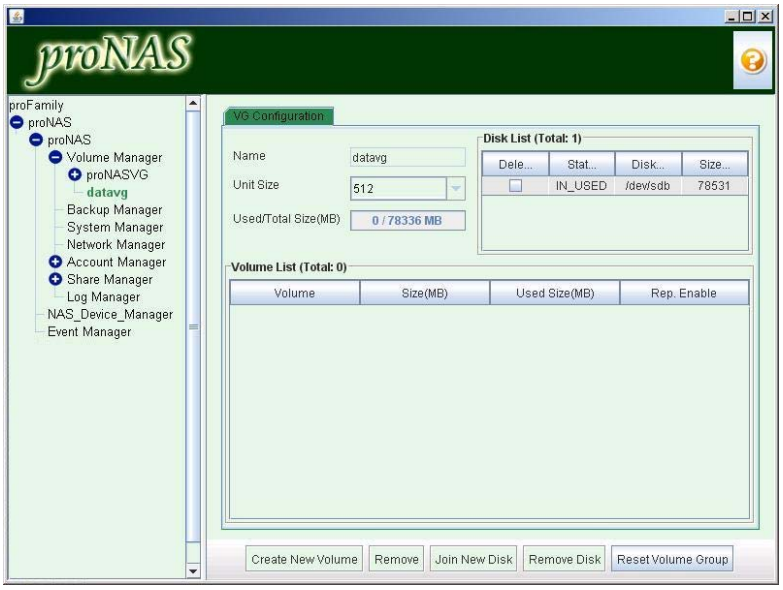
NOTE: The new VG has no default Logical Volumes. Admin can create new Logical Volumes.

NOTE: The NAS supports up to 5 Volume Groups. Volume Group is the highest level abstraction used within the NAS system. It gathers together a collection of Physical Volumes (consisting of at least one disk device, such as /dev/sda) and Logical Volumes into one administrative unit.

8.1.1.3 Reset and Remove Volume Group

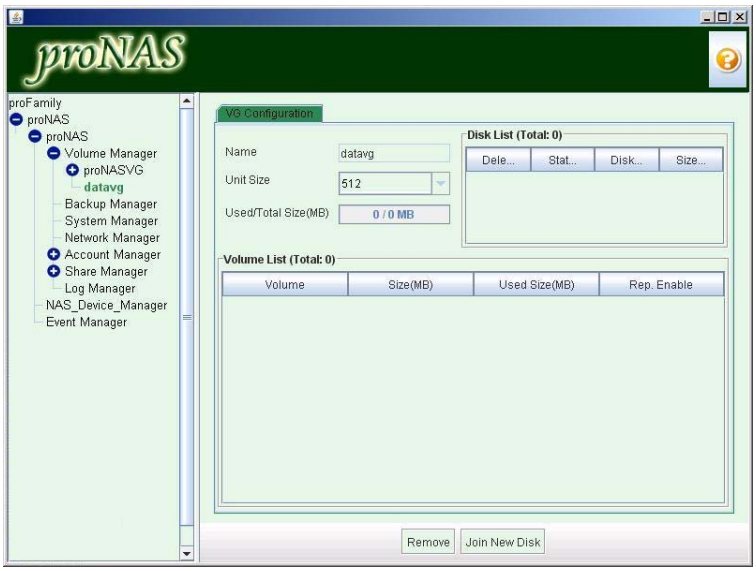
If you choose to reset the Volume Group, all the data will be erased. Use the “Reset Volume Group” function only when necessary, and when the data from the VG have been backed up or you do not want to keep the data.

1. Select “Reset Volume Group” button.



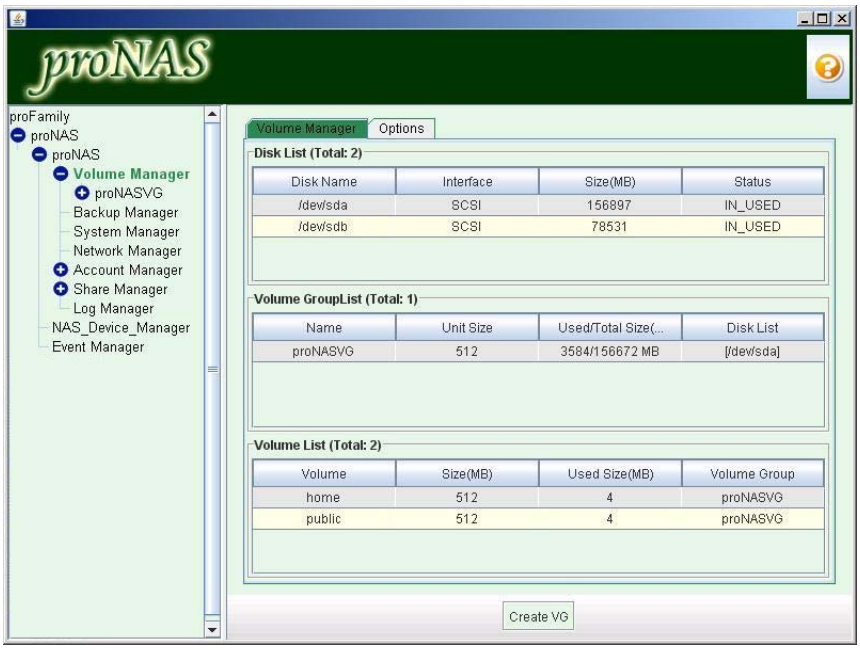
2. Select “Yes” to confirm.

3. Click “Remove”.



4. Select “Yes” from the confirmation message.

5. Verify from Volume Group List in Volume Manager that the VG has been removed.



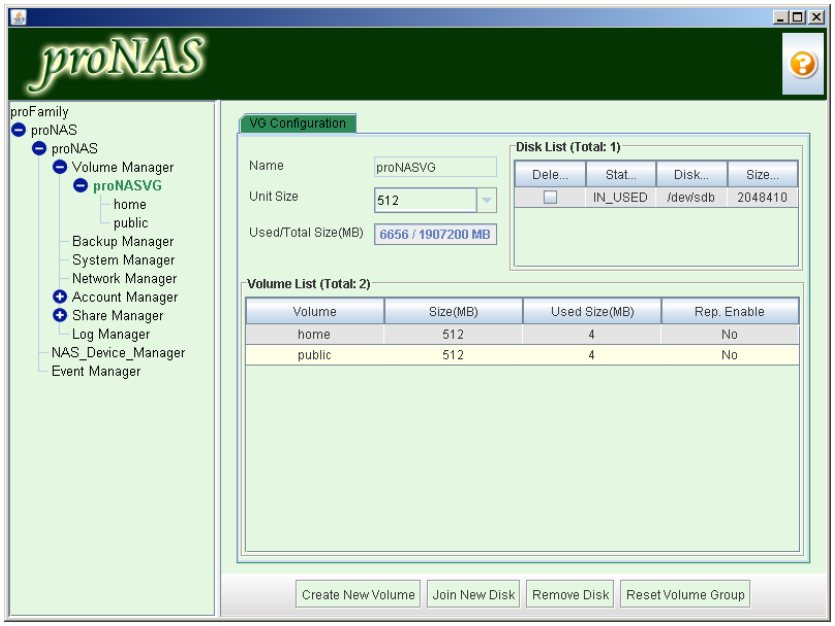
NOTE: The system default Volume Group “proNASVG” cannot be deleted or reset.

8.1.2 Logical Volume Configuration

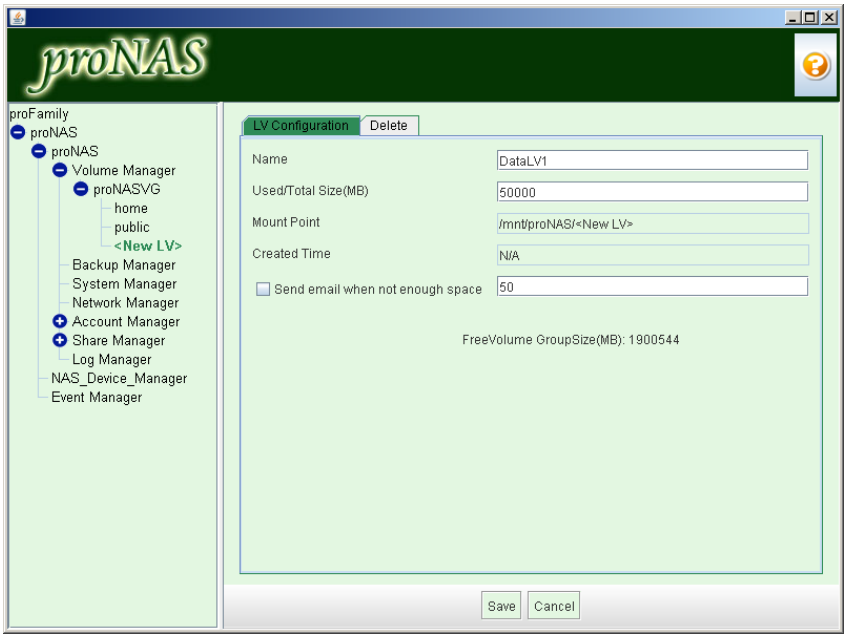
8.1.2.1 Create new Logical Volume

To create a new Logical Volume, follow these steps:

1. Double-click on a VG name. Click “Create New Volume” button.



2. The LV Configuration tab will be displayed. Enter the Logical Volume name and the volume size (in MB). You can also enable the “Send email when not enough space” option to send an email notification to email recipients specified in Event Manager if the remaining free volume size is smaller than the size entered in this option. Click “Save” when done.

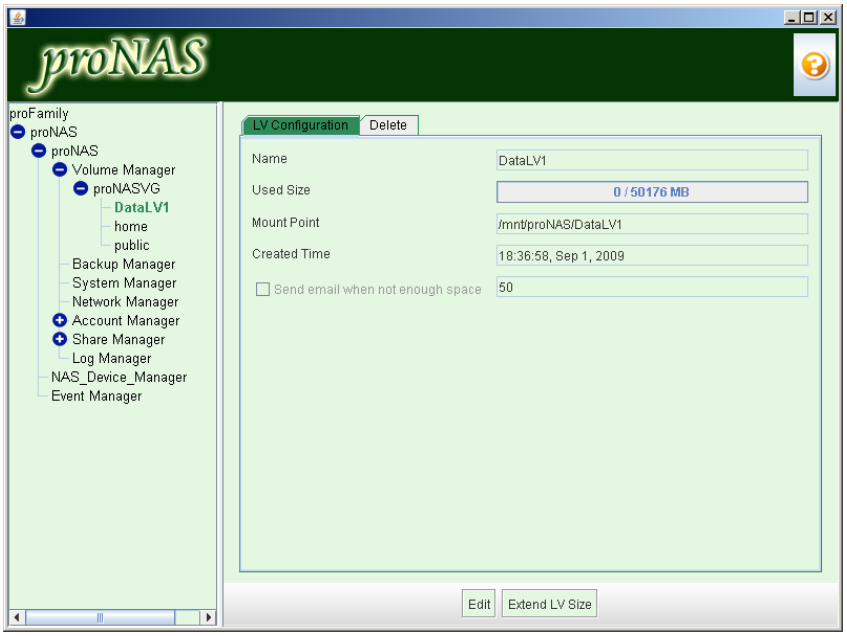


NOTE: The maximum LV size supported by proNAS 1.3.xx is 8 exabytes (EB) or 8 billion gigabytes. If the LV will use Replication, the LV size must be set to 16TB (the maximum LV size supported by Replication function).

3. Select “Yes” from the confirmation message to create the LV.

4. A process window will be shown.

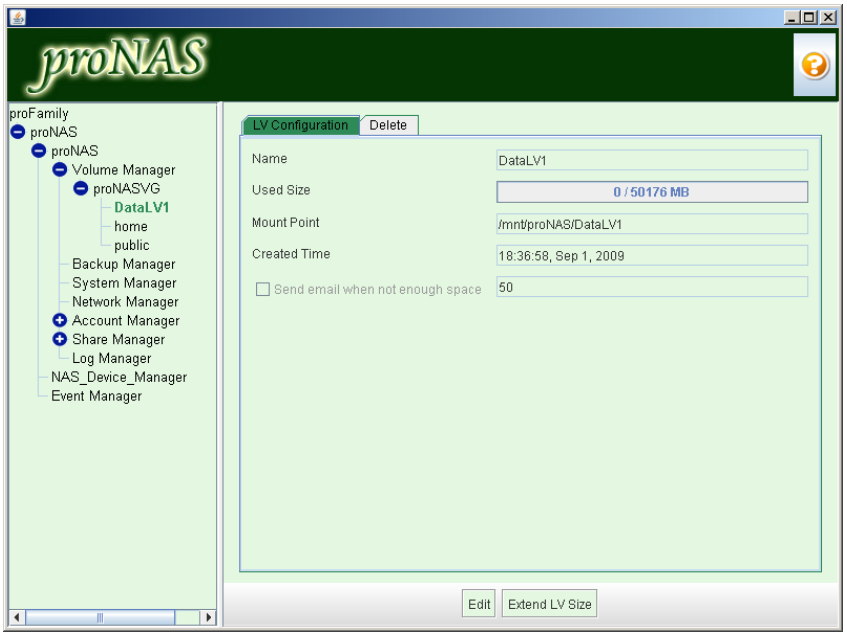
5. The new Logical Volume will be shown.



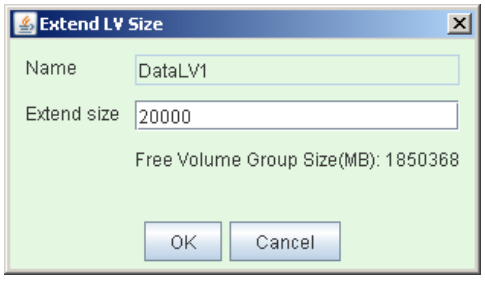
8.1.2.2 Extending Logical Volume Size

When the Logical Volume free space gets smaller and smaller, the Logical Volume size can be extended to allow more space for storing data. To extend the LV size, follow these steps:

1. Select the LV that will be extended then click “Extend LV Size” button.

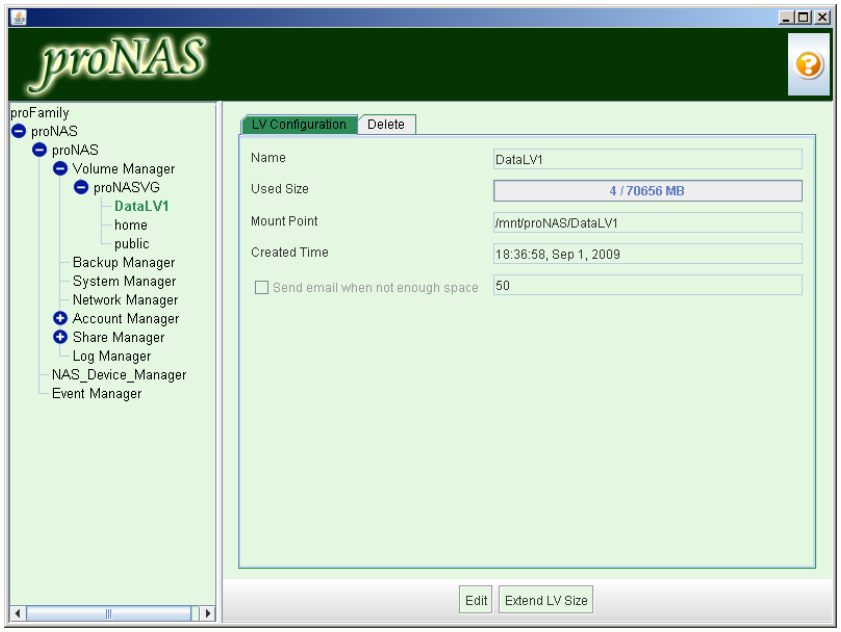


2. Enter in the “Extend size” box the additional size to be used for extension. Verify from the Free Volume Group Size (MB) the allowable size to be used in extension.



3. The Logical Volume will be extended.

4. Verify the new LV size.



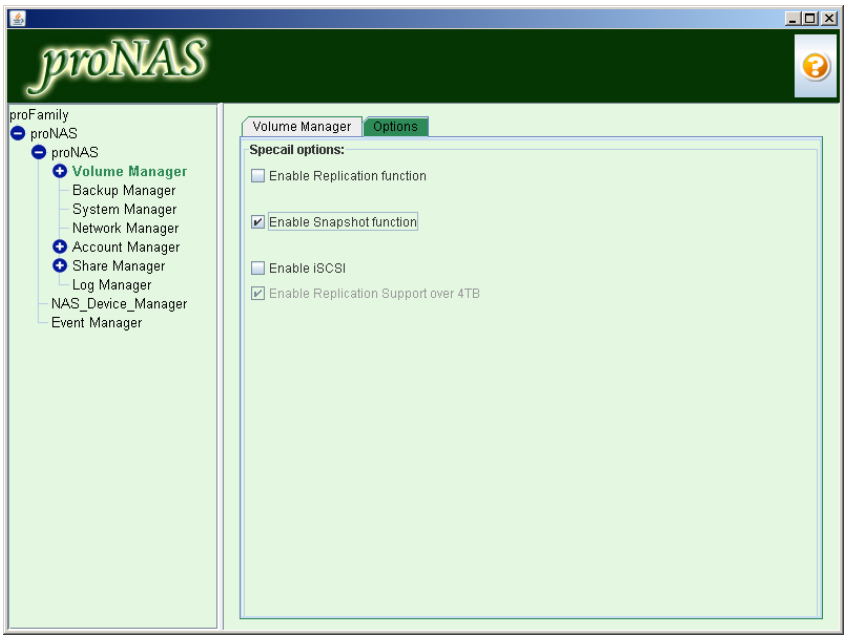
8.1.3 Volume Snapshot

Snapshots are point-in-time copies of a logical volume. This allows the system administrator to create a new block device which presents an exact copy of a logical volume, frozen at some point in time. As changes are made to the original volume, the snapshot remains the same and looks exactly like the original at the time the snapshot was created.

A Snapshot can be created manually or scheduled. Admin need to enable first this special function.

NOTE: Logical Volume with snapshot cannot be extended nor replicated (see next section about Volume Replication).

To enable Snapshot function, select Volume Manager then click Options tab. Tick the “Enable Snapshot function” option.

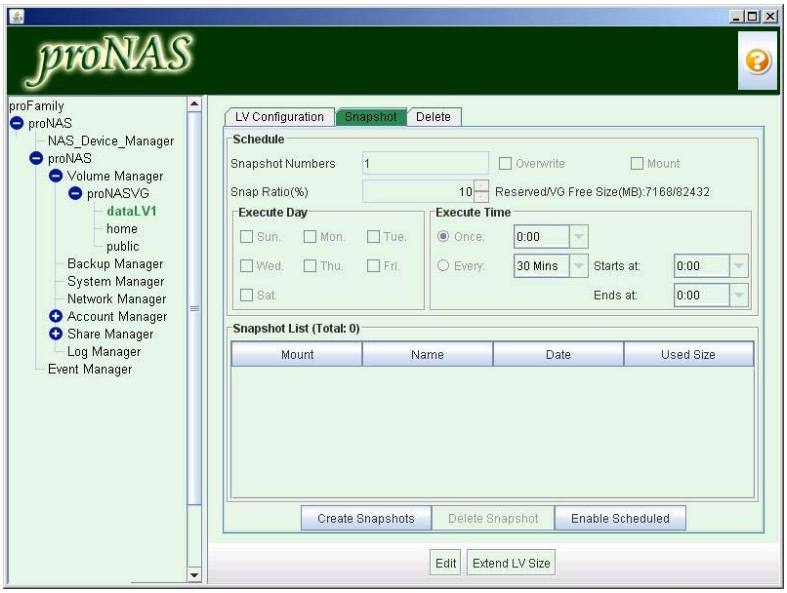


NOTE: Creating Snapshots while a Logical Volume is under heavy I/O will slowdown the I/O access or interrupt the I/O process to a Logical Volume. This means that clients accessing the proNAS share, in which the Logical Volume is under snapshot, can experience slow write access.

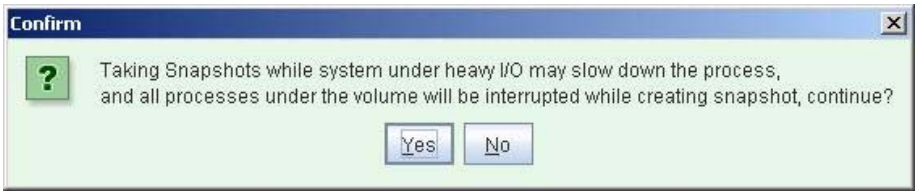
8.1.3.1 Create Snapshots Manually

To manually create snapshots:

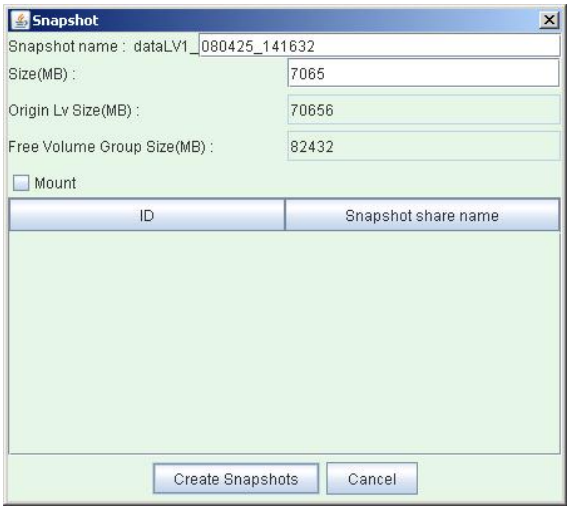
1. Select the Logical Volume, go to Snapshot tab and click “Create Snapshot”.



2. A confirmation message will appear. Select “Yes”.


Confirm
Taking Snapshots while system under heavy I/O may slow down the process,
and all processes under the volume will be interrupted while creating snapshot, continue?
Yes
No

3. The Snapshot configuration window will be displayed. A system-created Snapshot name is automatically created. The default snapshot name can be renamed if needed. Enter the new Snapshot Size (in MB) if the size shown need to be changed. See details about Snapshot Options below. Click “Create Snapshots” to start creating snapshot.

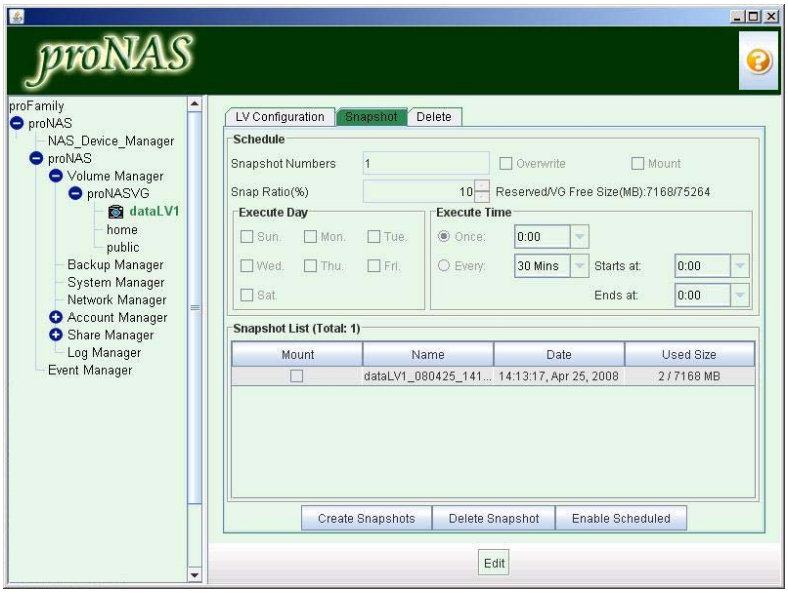


Snapshot Options:

- **Snapshot Name:** The default snapshot name is created by appending the date and time to the volume name. You can modify the snapshot name but the prefix volume name will still remain.
- **Size (MB):** This indicates the size of the snapshot volume that will be created. The default is 10% of the size of the logical volume where snapshot is to be taken. The size of the snapshot volume will be multiple of the PE size.
- **Origin LV Size:** This indicates the size of the Logical Volume where the new snapshot volume will be created.
- **Free Volume Group Size (MB):** This indicates the amount of free space on the volume group where the new snapshot volume will be created.
- **Mount:** When checked, the created snapshot volume will be automatically mounted. When a snapshot volume is mounted, the existing share from the snapshot volume will be accessible. Note that a snapshot volume is a read-only volume.
- **ID:** This specifies the shares created under this logical volume.
- **Snapshot share name:** This specifies the name of the snapshot shares. Your may access these shares by mounting the snapshot volume. The naming format used is: the last two digit of the year, followed by the month/date, and then followed by the hour/min/sec. For example: "060123_171516".

4. A process window will be displayed.

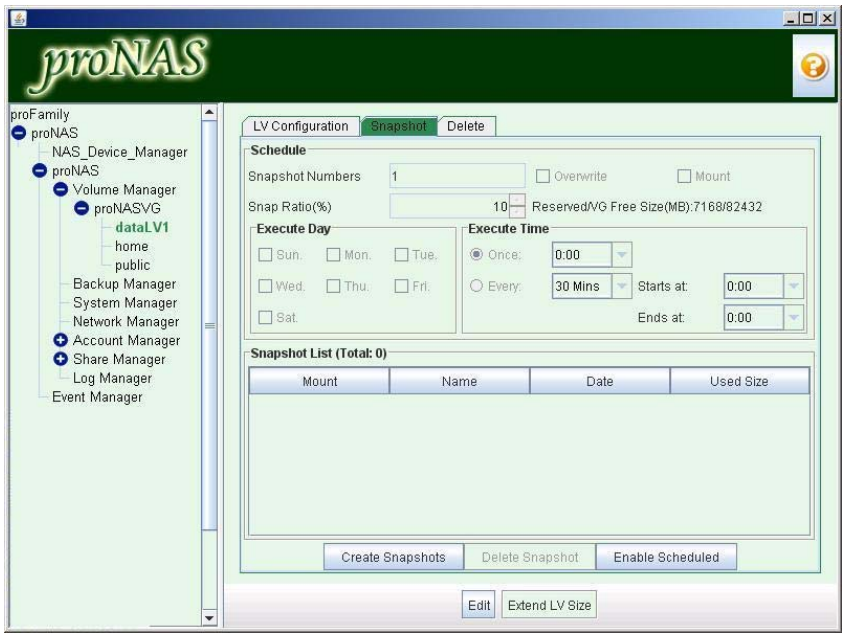
5. When snapshot has been created, it will be shown in the Snapshot List of the Logical Volume.



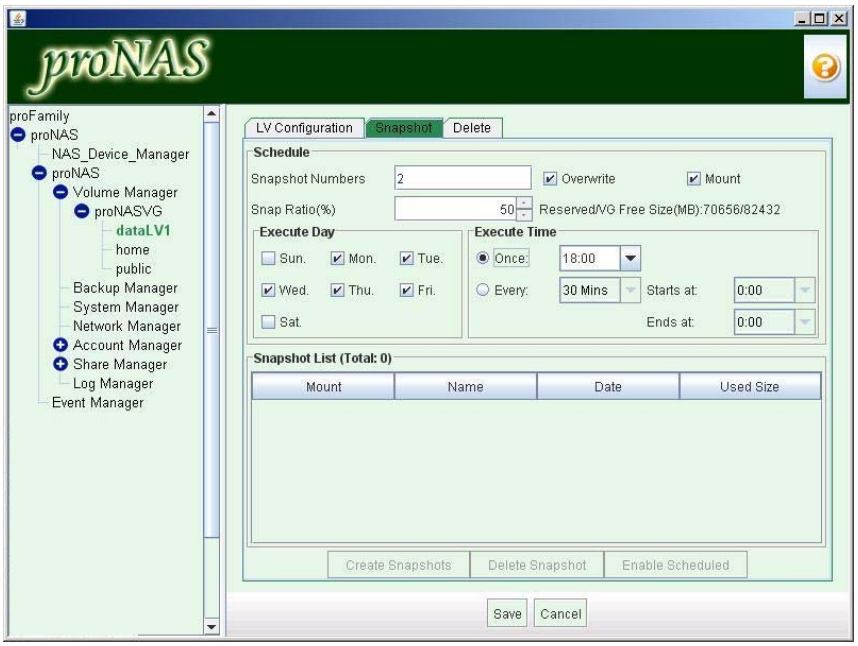
8.1.3.2 Create Snapshots Based from Schedule

To create scheduled snapshots:

1. Select the Logical Volume, go to Snapshot tab and click “Edit”.



2. Edit the following snapshot options listed below then click “Save” when done.



Snapshot Options:

- **Snapshot Numbers:** Specifies the total number of snapshots that will be created.
- **Snap Ratio (%):** This is the ratio in percentage between the snapshot volume and the volume of origin. This indicates the ratio of the volume size that will be set as the size of the snapshot volume. For example, if your logical volume is 1GB and the Snap Ratio is 10%, the size of the snapshot volume that will be created is 128MB, assuming that your PE size is 128MB and below. The snapshot volume size will always be a multiple of PE size and the smallest snapshot size is equal to the PE size.
- **Overwrite:** Selecting this option will automatically delete the oldest snapshot if the total number of snapshots is already exceeded.
- **Mount:** When checked, it means that the created scheduled snapshot will be automatically mounted.
- **Reserved/VG Free Size (MB):** The left side indicates the total volume space that will be used for the creation the snapshots. The right side indicates the free space of the volume group available for use.
- **Execute Day:** Specifies whether the scheduled task is to run on the selected day(s).
- **Execute time:**

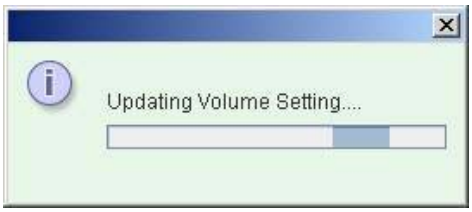
  Once - Specifies the time of the day when the scheduled task will be taken.
  Every - Specifies how often the scheduled task is to be repeated. You can also select the starting time and the ending time.

- **Snapshot Lists:**

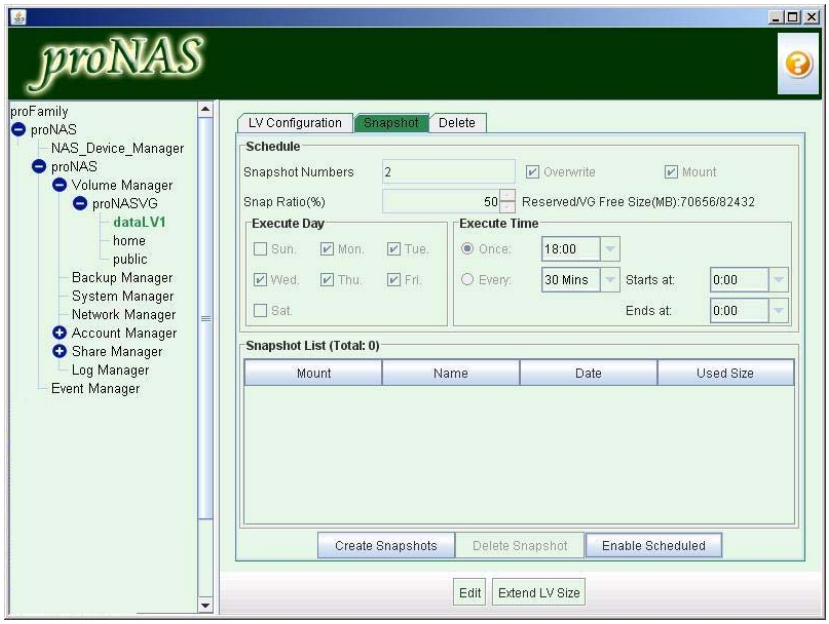
  Mount - Allows you to mount the snapshot volume. All snapshot volumes will be mounted read-only. By mounting the snapshot volume, the files under this snapshot volume will become accessible.
  Name - This specifies the name of the snapshot volume. If the snapshots are created by schedule, proNAS will automatically create the snapshot name. The format that will be used is: the last two digit of the year, followed by the month/date, and then followed by the hour/min/sec. For example: "060123_171516".
  Date - This indicates the date and time when the snapshot was created.
  Used Size - This indicates the space used by the snapshot data. The right side is the size of the snapshot volume. If the used space nearly exceeds the snapshot volume capacity, it will be set as "Invalid" and will be un-mounted automatically to keep the system consistent.

3. A confirm message window will be displayed. Select “Yes” to proceed.

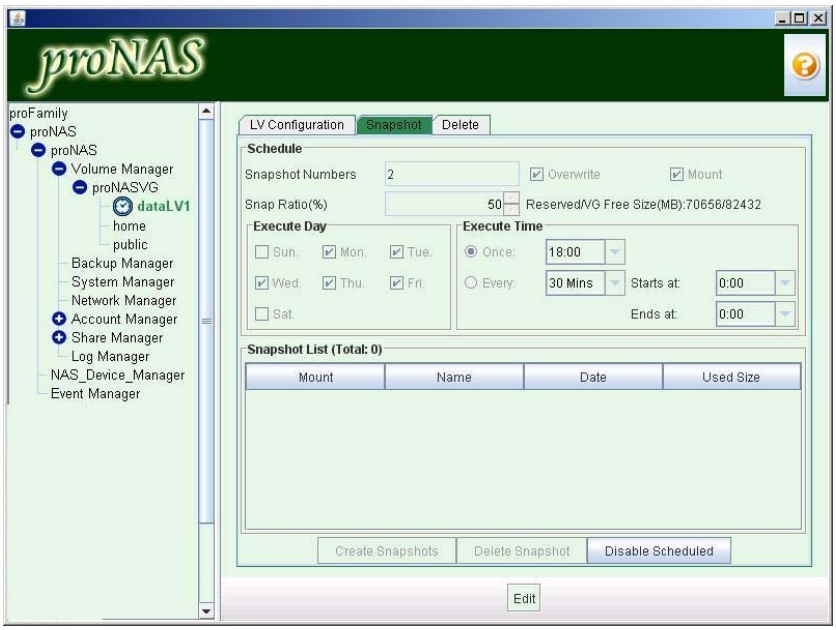
4. An “Updating Volume Setting” message will be shown.



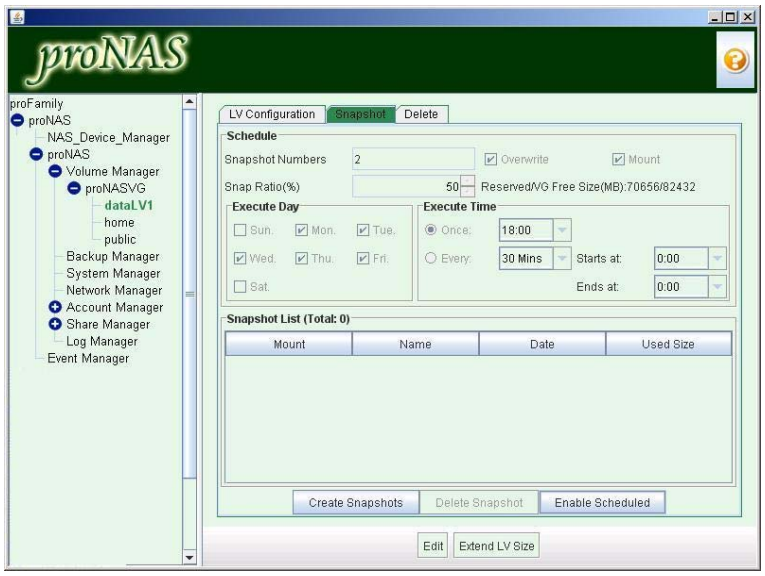
5. When the snapshot setting of LV has been set, click “Enable Scheduled” to active scheduled snapshot.



6. A clock-like icon will appear on the left side of the LV which means a scheduled snapshot is active. To disable the schedule, click “Disable Scheduled”.

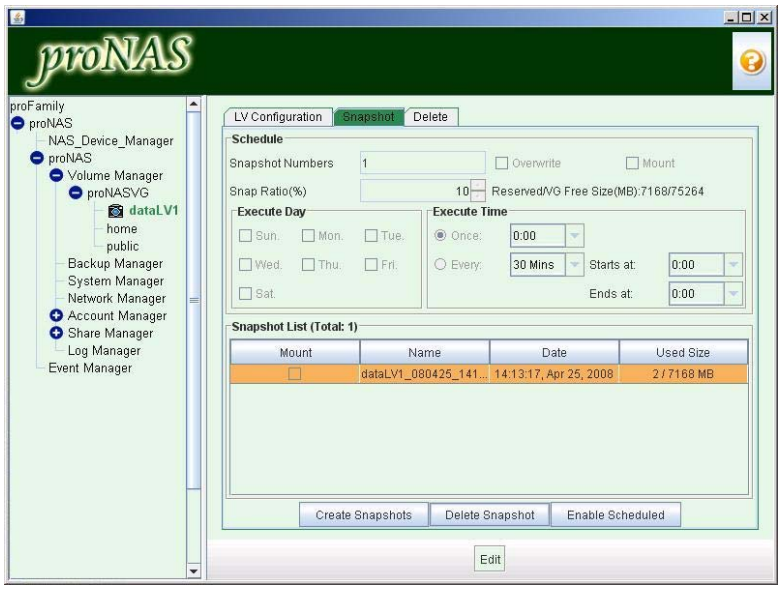


7. After disabling the schedule, the “Enable Scheduled” button will become available.



8.1.3.3 Delete Snapshots

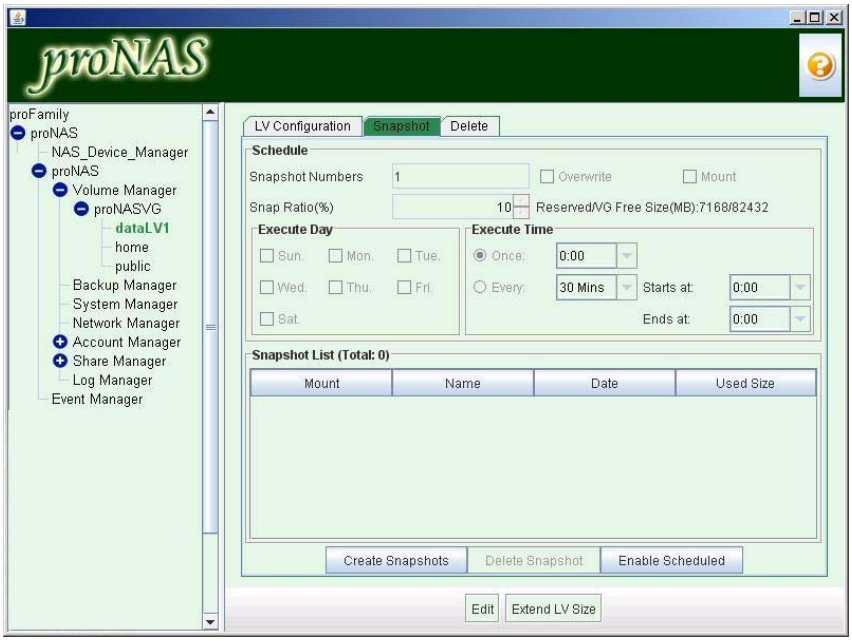
1. Select the Logical Volume where snapshot will be deleted, then go to Snapshot tab. Click the snapshot that will be deleted then click “Delete Snapshot”.



2. Select “Yes” to delete the snapshot.

3. A process window will be shown.

4. The deleted snapshot will no longer exist in the Snapshot List.



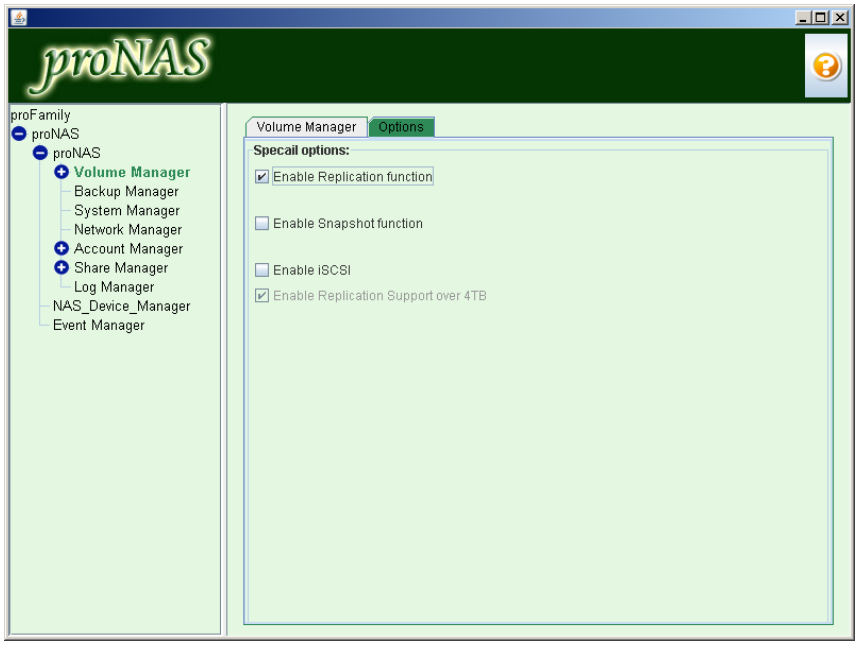
8.1.4 Volume Replication

Replication function enables proNAS to replicate a logical volume from one NAS server (source) to another NAS server (destination). Replication involves intelligent copying and maintaining of exact copy of a volume from a source server to a destination server. The destination volume is always an exact copy of the source volume. This is done by mirroring the whole block device via a standard network interface. This solution creates a real time replication of data. However, it does not create a cluster solution where you can have a highly available system.

Note: Logical Volume under snapshot cannot be replicated.

NOTE: In proNAS version 1.3.xx, Replication of Logical Volumes with LV capacity up to 16TB is supported.

To enable Replication, select Volume Manager then click Options tab and tick “Enable Replication function”.

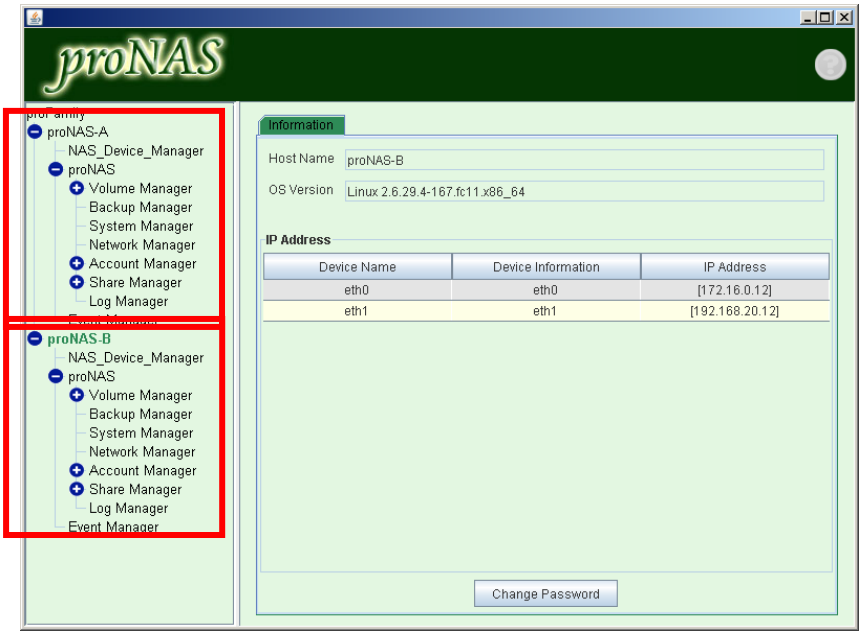


NOTE: Make sure the two proNAS servers have different host names before setting up Replication.
It is advisable to configure a network port, in each of the two NAS servers, as dedicated channel/medium for Replication.

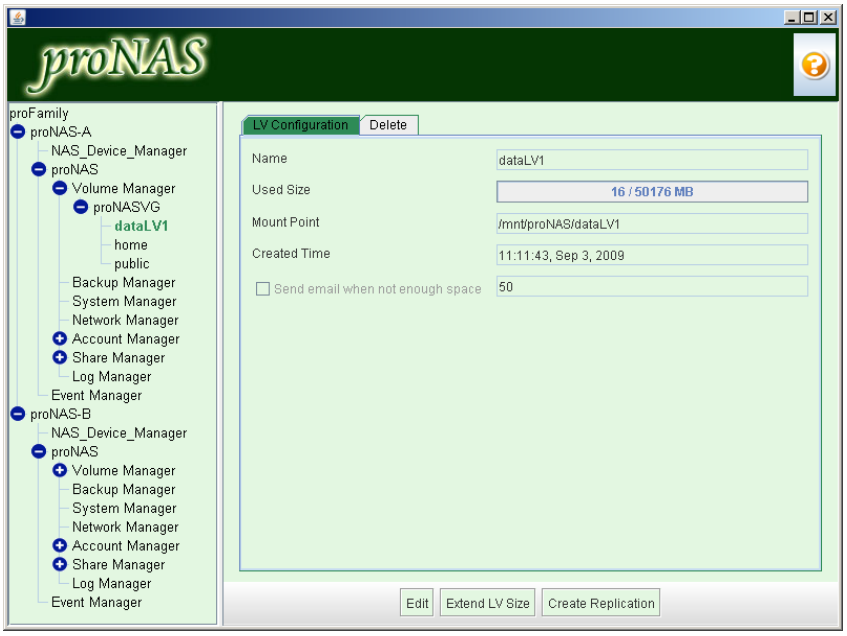
8.1.4.1 Replication Configuration

To setup Replication between two NAS servers:

1. Admin need to login to the administration page of the two NAS servers.

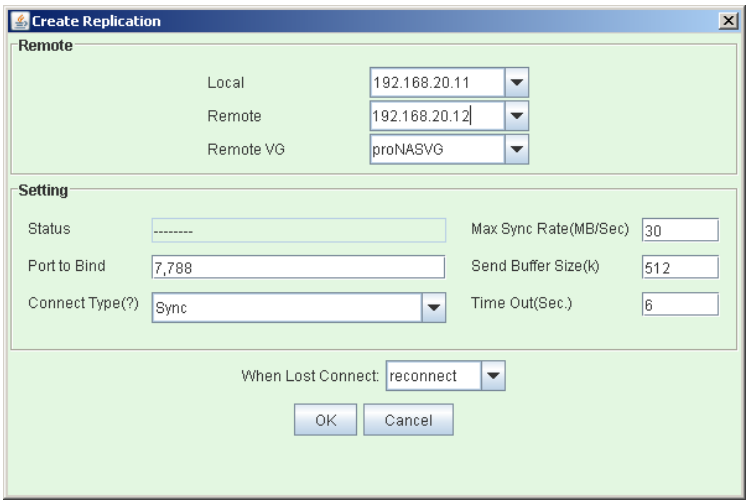


2. On the primary NAS (source), select the Logical Volume which will be replicated, then click “Create Replication”.



NOTE: The logical volume to be replicated from source proNAS must not exist in the destination proNAS. If the destination proNAS has the same logical volume, replication cannot be setup.

3. The Create Replication window will be displayed. Set the options below and click "OK" when done.



Replication Options:

[Remote]

- **Local** - Select the IP address of the local (source) proNAS that will be used for replication.
- **Remote** - Select or type manually the IP address of remote (destination) proNAS that will be used for replication.

NOTE: The local and remote IP addresses serve as the channel between the source and destination NAS servers. This is where the replication of data takes place. Please be sure to have a good connection on this medium. As much as possible, set this channel as a dedicated or a private network. It is recommended to use different Ethernet port for replication from the Ethernet port used for data access. It is best to use a crossover network link between the Ethernet ports involved. Refer to Network Manager Section for configuring Ethernet port.

- **Remote VG** - Select the VG on remote proNAS where the replicated logical volume will be created.

[Setting]

- **Port to Bind** - A TCP port to bind locally and is used to connect to the remote node. Default is 7788.

NOTE: User cannot use ports that already have been used. Available ports are from 7788 to 77xx.

- **Connection Type:** proNAS supports two types of data replication protocols:
  - **Sync** - Synchronous. The system will acknowledge the transaction as completed after the data is written to the disk of destination proNAS. It is recommended to use this mode. In most cases, this connection type preserves transaction semantics. Write IO is reported as completed if it has reached the remote disk.
  - **Async** (for high latency network) - Asynchronous. The system will acknowledge the transaction as completed after the data is written to buffer. It provides faster transmission and is suitable for busy network. Write IO is reported as completed if it has reached the local TCP send buffer.
- **Max Sync Rate** – This sets the limit of the bandwidth that will be used by the synchronization process. Default is 30MB/sec. Minimum value is 4MB/sec and maximum value is 680 MB/sec – for high latency network environment (e.g. bonding on Gigabit Ethernet).
- **Send buffer size (K)** - It is the size of the TCP socket send buffer. You can specify smaller or larger values. Larger values are appropriate for reasonable write throughput with asynchronous protocol over high latency networks. Default is 512K and maximum is 1024K.
- **Time out (sec)** - It is the value to wait for connection timeout if the remote node is degraded. If the remote node fails to send the response packet within the specified timeout time, the remote node will be considered dead and the TCP/IP connection is abandoned. The default is 6 sec. Minimum is 1 sec and maximum is 60 sec.

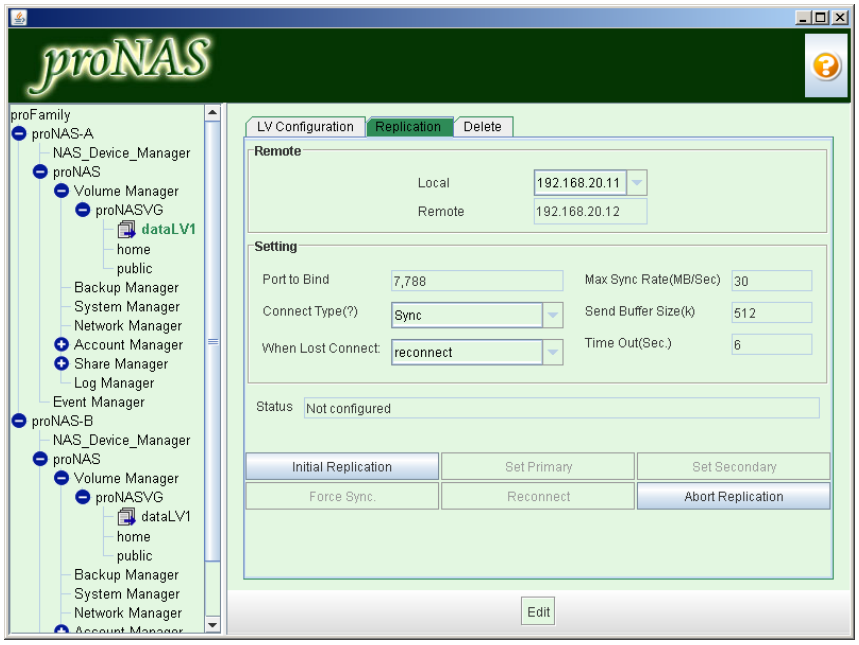
- **When Lost Connection**: When the replication connection is lost, the replication program can either go stand-alone or will try to reconnect.

  - **Reconnect:** The replication program will attempt to reconnect. (Default)
  - **Stand-alone:** The replication program will not attempt to reconnect and will go on stand-alone state. All IO request are only passed locally and no replication.

NOTE: Before replication will be successfully created, a 4GB logical volume will be created on each node. This will serve as the metadata device for the replicated volume. This volume is not mounted and will not be seen on the proNAS GUI. Please be sure to have an extra 4GB space on either side of your NAS nodes.

4. A message box will be displayed. When completed, Replication is enabled in the LV.

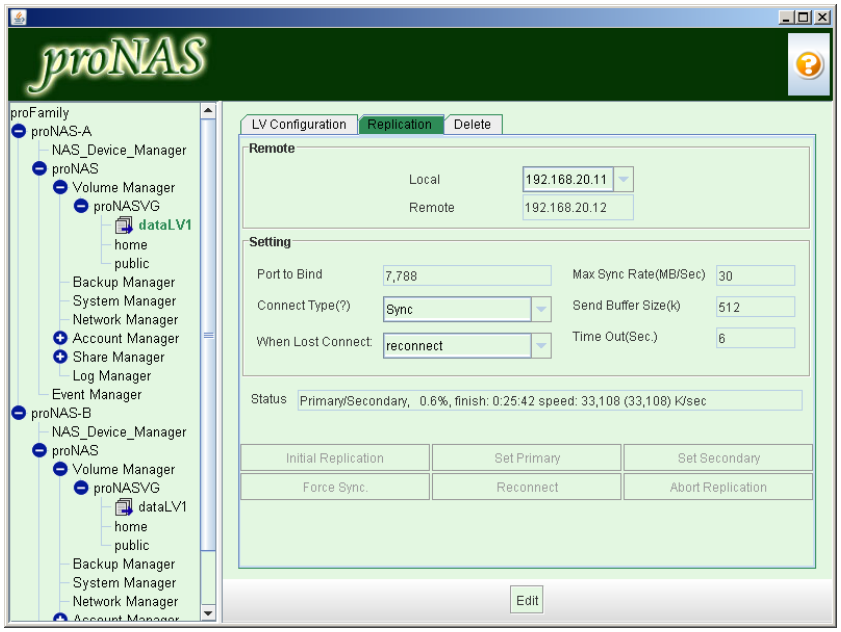
5. Select the LV name, then click Replication tab. Initialize the Replication by clicking "Initial Replication" button. When the confirmation message is displayed, select "Yes" to continue.



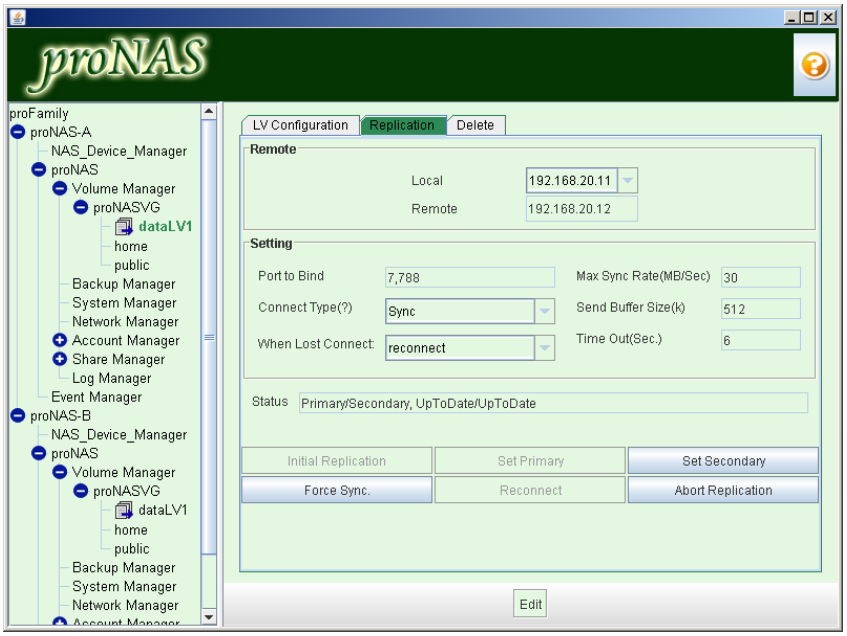
NOTE: After creating Replication on a logical volume, a similar logical volume will be created on the destination server under the specified VG. At this point, the Replication is not yet initialized and no synchronization. Replication still needs to be initialized. After selecting "Initial Replication" button, the first node will then connect to the second node and starts to synchronize. Synchronization typically takes quite a while especially on larger logical volumes. After initializing, the source node should be in "Primary" state and the destination node should be in "Secondary" state. If this is the state, you have now a working replication. Initializing should be done in the source volume.

6. The volume replication setting will be initialized.

7. The volume replication synchronization process will start.



8. After the initial synchronization process is completed, the Status will show "Primary/Secondary, UpToDate/UpToDate".



8.1.4.2 Checking the Status of Replication

Primary: The node of source volume. All the writing and reading are done on the primary node.

Secondary: The node of destination volume. The replicated data on the secondary node is used for backup only and is not accessible. Only the source data is accessible during replication.

Unknown: The node fails to establish connection.

UpToDate: The node is updated.

Setting the replicated volume on destination proNAS to be Primary

To set the replicated volume to primary, first you need to set both nodes to secondary. This can be done by setting the primary to be secondary. After both nodes becomes secondary/secondary, go to the management GUI of the destination node. Under the replicated logical volume, press the "Set Primary" button.

WARNING! The replicated volume on the secondary node must not be mounted. Please do not attempt to mount it manually.

Setting the primary volume to be secondary

To set the primary volume to be secondary, just press the "Set Secondary" button on the primary node.

Forcing the synchronization

To manually force the synchronization, press the "Force Sync." button. The data on the primary node will be forcefully synchronized to the secondary node.

Reconnect when the connection of the peer is lost.

To reconnect the replicated volume, press the "Reconnect" button. At some point if the replication fails to establish connection to the other node, you may try to set up a connection thru this button. This button will be enabled only if one of the node losses connection.

Aborting the replication

To abort or drop the replication, press the "Abort Replication" button. To access the data on the replicated volume after aborting the replication, you may need to create a share under destination volume whose share name must be equal to the share name on the source proNAS.

8.1.4.3 Extending Logical Volume under Replication

NOTE: Extending the size of a Logical Volume under Replication is not allowed. However, there is a work around to extend the LV size. Note that the extended LV size must not exceed 16TB.

The following are the steps:

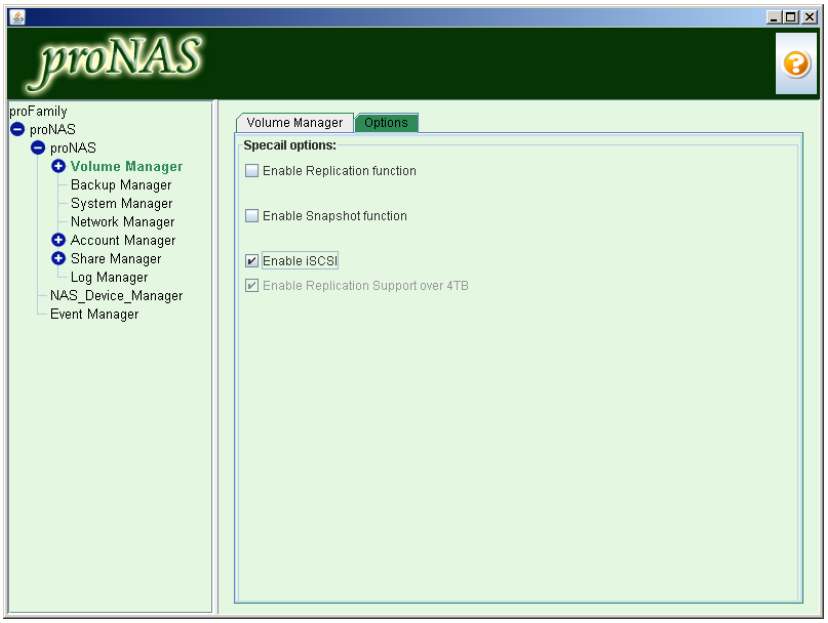
1. Abort the replication by selecting “Abort Replication”.
2. Remove or delete the replicated logical volume on the destination proNAS.
3. Extend the capacity of the source logical volume. Please note that there should be enough space on the VG of the destination proNAS to accommodate the extended logical volume space.
4. Create a new Replication using the extended source logical volume.

8.1.5 iSCSI

The iSCSI function in proNAS makes a logical volume become an iSCSI target LUN.

Note: You can't enable iSCSI function in a Logical Volume if Snapshot or Replication exists.

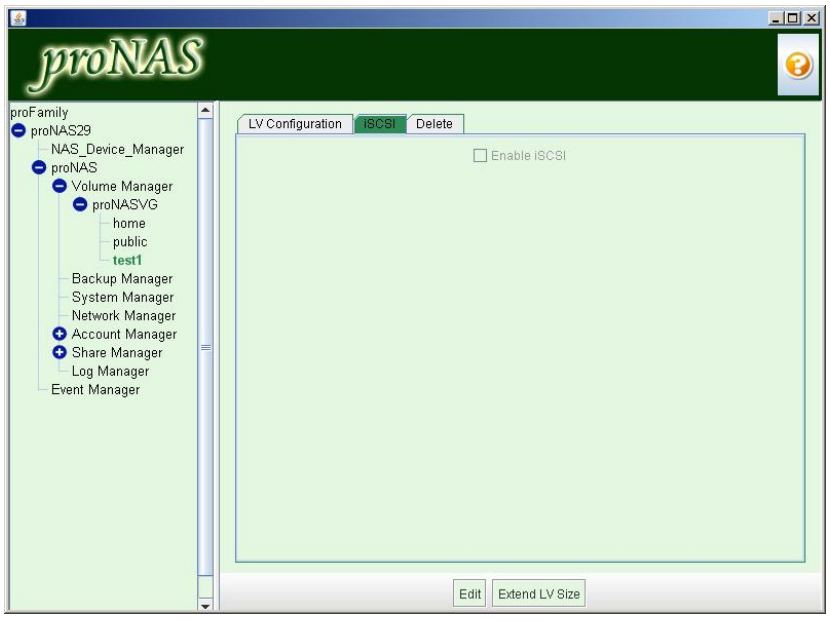
To enable iSCSI function, select Volume Manager then click Options tab and tick "Enable iSCSI".



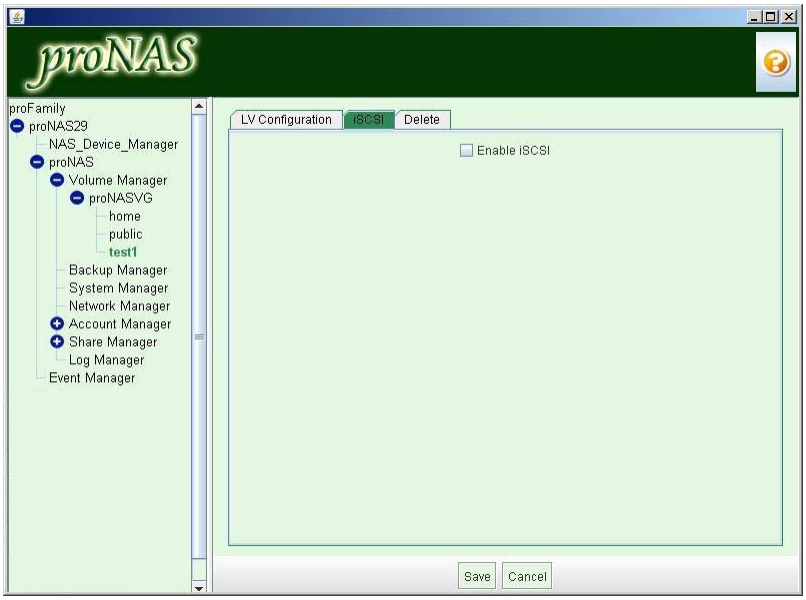
8.1.5.1 iSCSI Configuration

To configure iSCSI:

1. Select the logical volume and click the iSCSI tab.

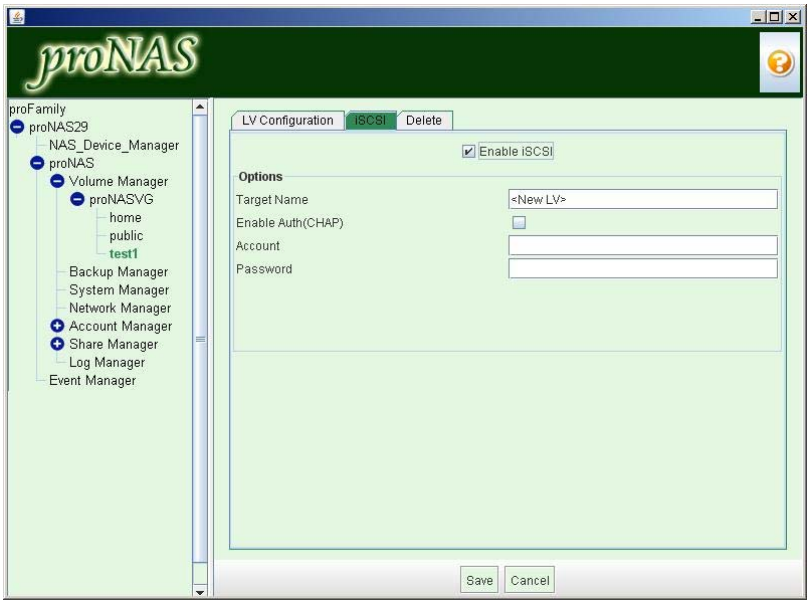


2. Click “Edit” and tick the “Enable iSCSI” option.

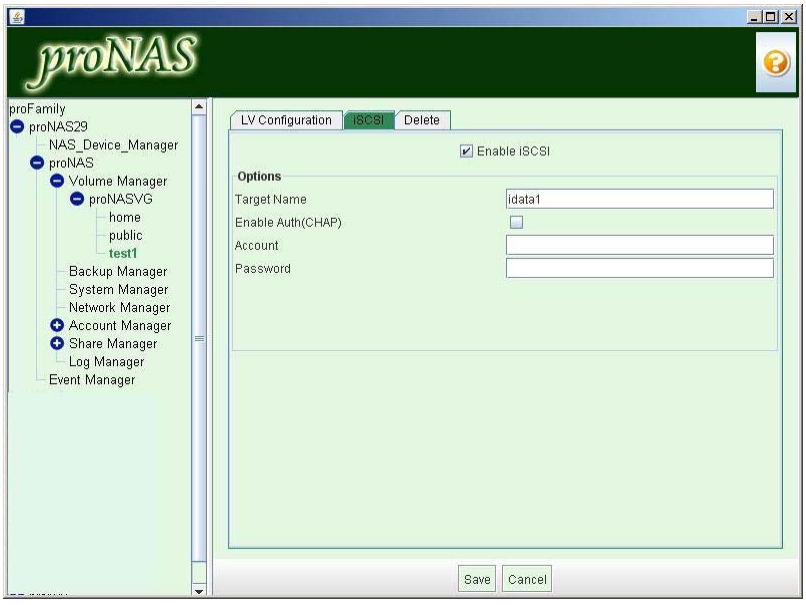


3. Enter the iSCSI target name. If you want to enable CHAP authentication, check the “Enable Auth (CHAP)” option and enter the account and password.

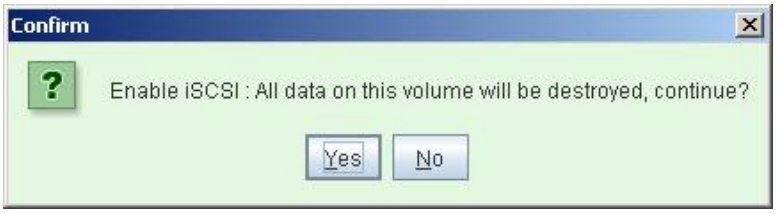
NOTE: Valid characters for iSCSI Target name are: a-z, A-Z, and 0-9. Other special characters and space are not allowed. CHAP Password must be 12 to 16 characters.



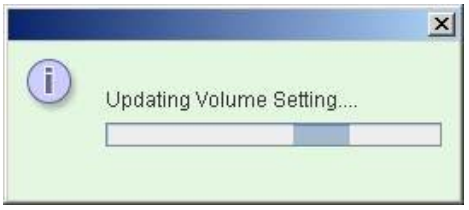
4. Click “Save” when done.



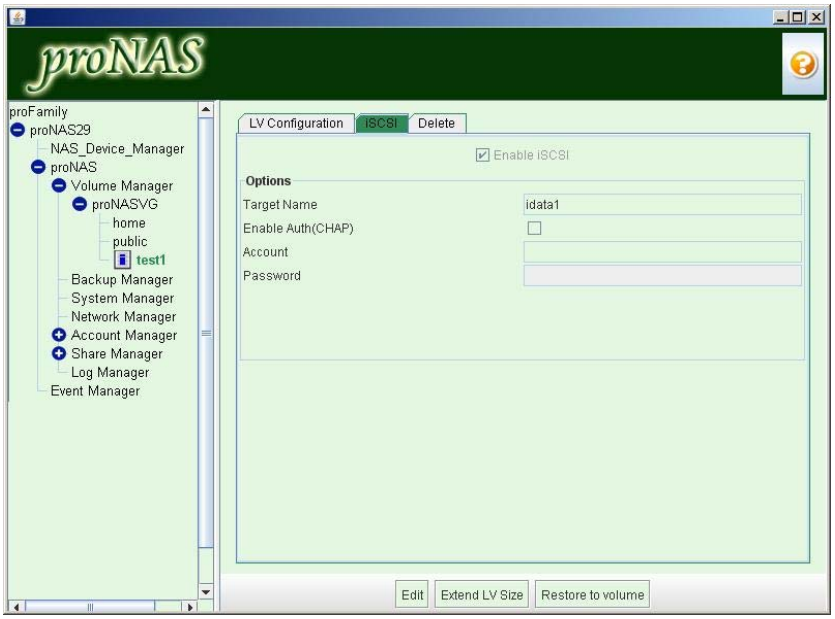
5. A message box will be displayed. Select “Yes” to continue.



6. A progress box will be displayed.



7. The iSCSI volume is ready. Note that there is an “**i**” icon on the left of logical volume name to denote that this is an iSCSI volume.



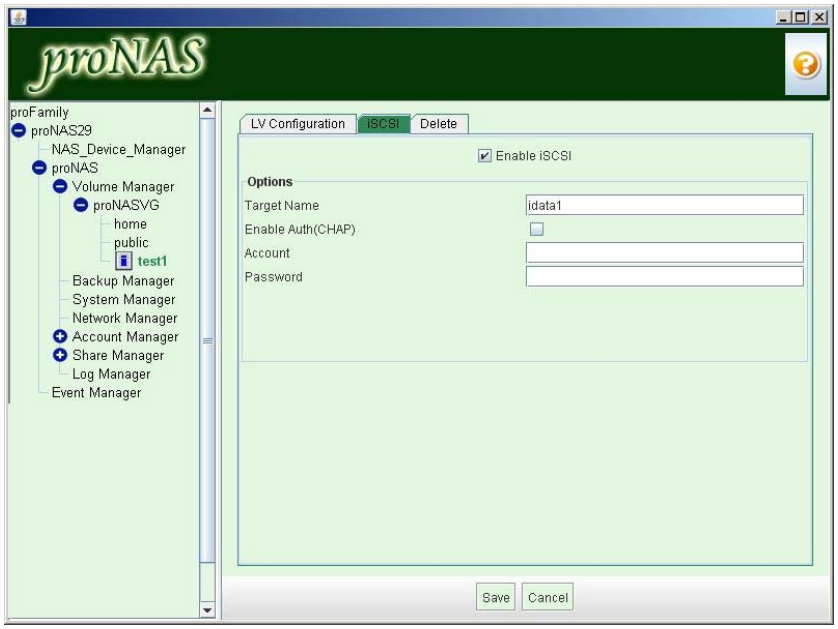
8. You may now connect to the iSCSI target LUN using iSCSI initiator.

8.1.5.2 Disable iSCSI in Logical Volume

To disable iSCSI:

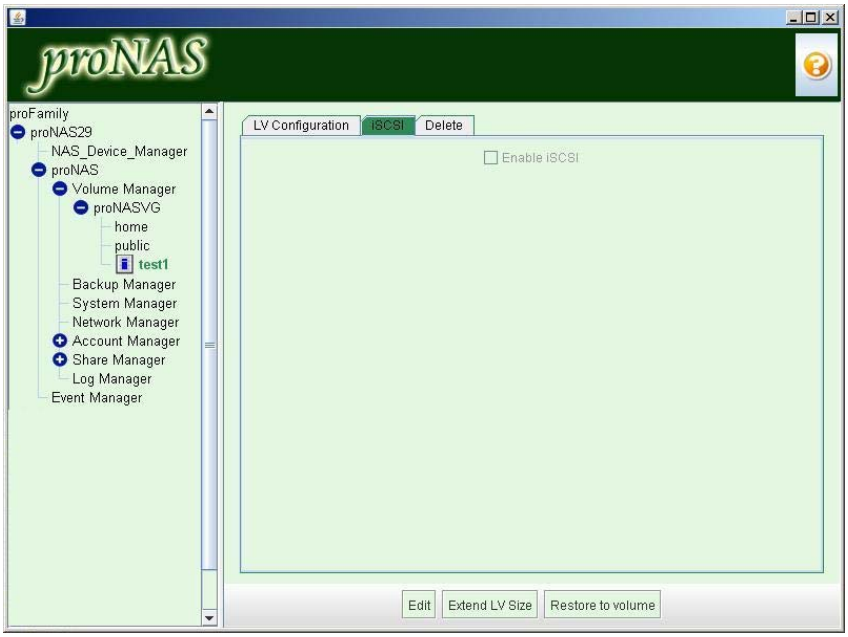
1. Select the logical volume and click the iSCSI tab.

2. Click “Edit” and remove the check mark in “Enable iSCSI” option. Click “Save” when done.



3. A confirm message box will be displayed. Select “Yes” to proceed.

4. The iSCSI function in the logical volume is disabled.

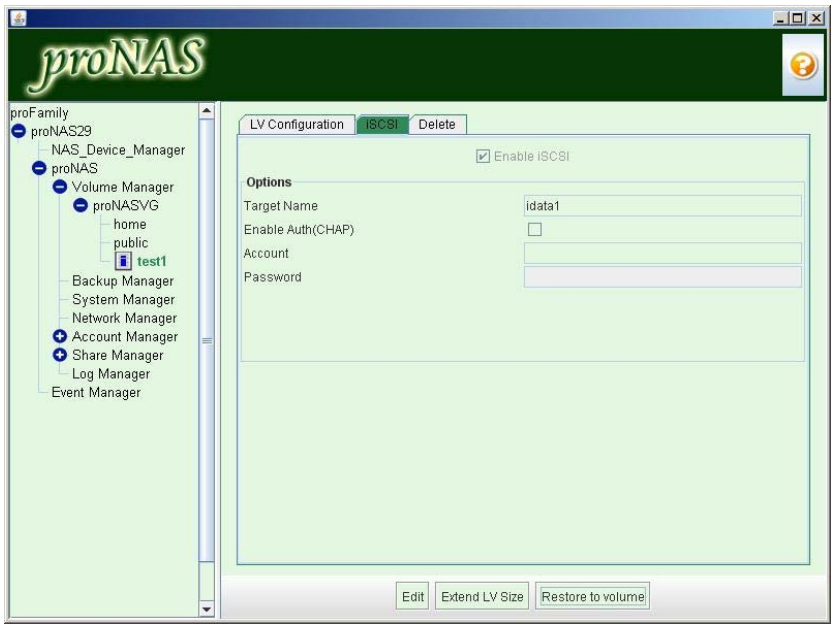


8.1.5.3 Restore iSCSI to Ordinary Logical Volume

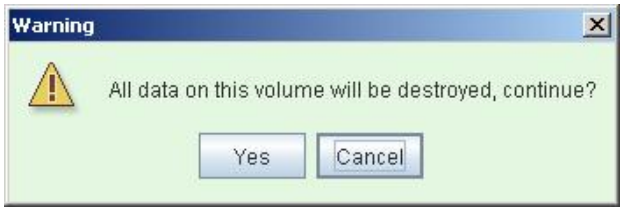
The iSCSI volume can be restored back to normal logical volume and remove the iSCSI function. The existing data in the logical volume will be deleted; so if there are important data in the logical volume, a backup must be made.

To restore iSCSI to normal volume:

1. Select the logical volume and click the iSCSI tab. Select the “Restore to Volume” button.

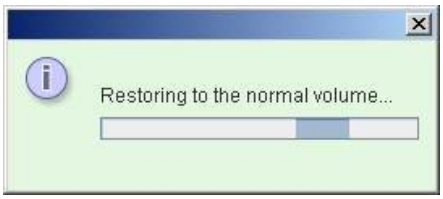


2. When a warning message is displayed, select “Yes” to proceed.

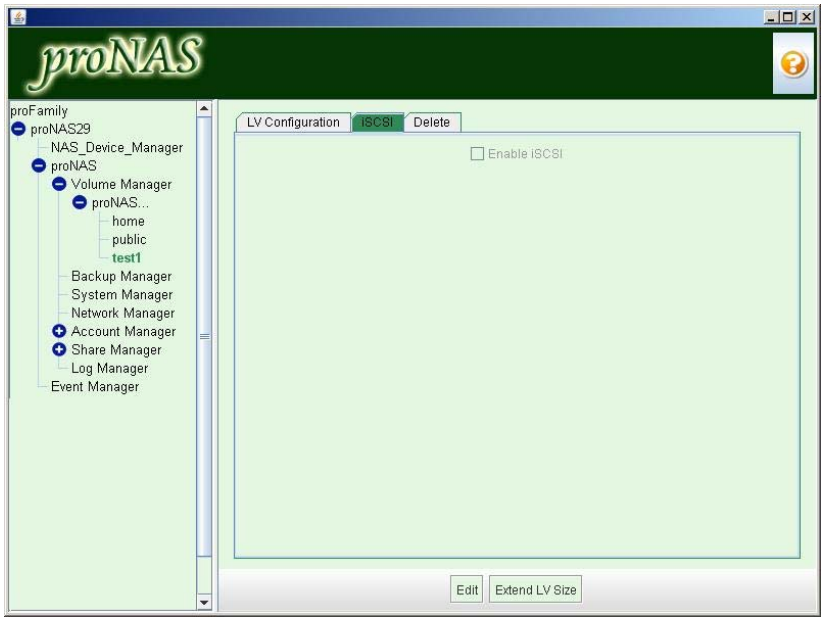


3. When a confirm message is displayed, select “Yes”.

4. A process window will show that the volume is being restored back to normal logical volume.



5. The logical volume is restored to normal volume. Note that the "**i**" icon on the left of logical volume name has been removed.

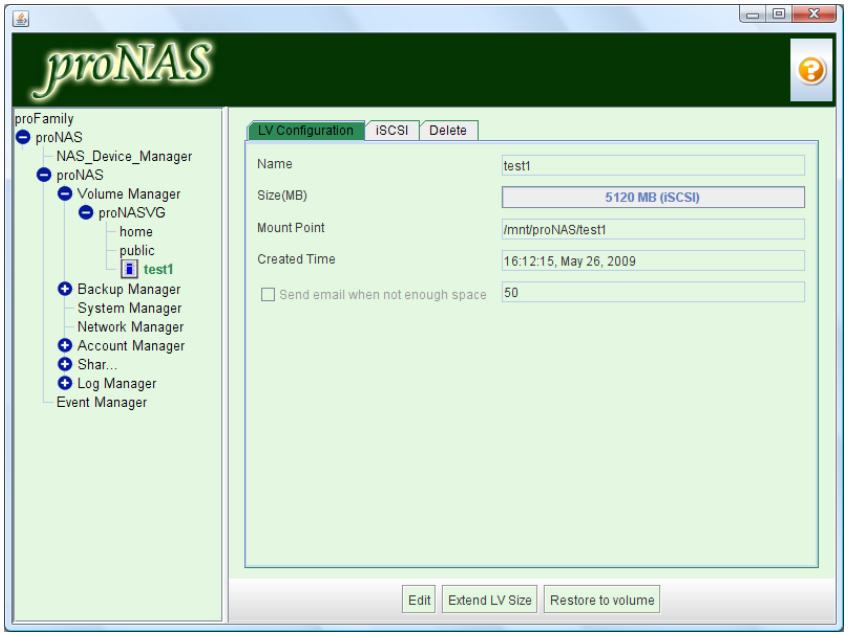


8.1.5.4 Extending iSCSI Logical Volume Size

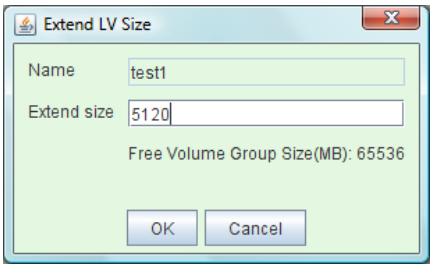
The capacity of iSCSI volume can be extended to allow more data to be stored.

To extend iSCSI volume capacity:

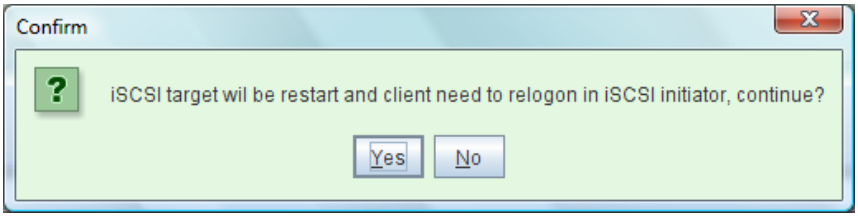
1. Select the iSCSI volume. Click “Extend LV Size”.



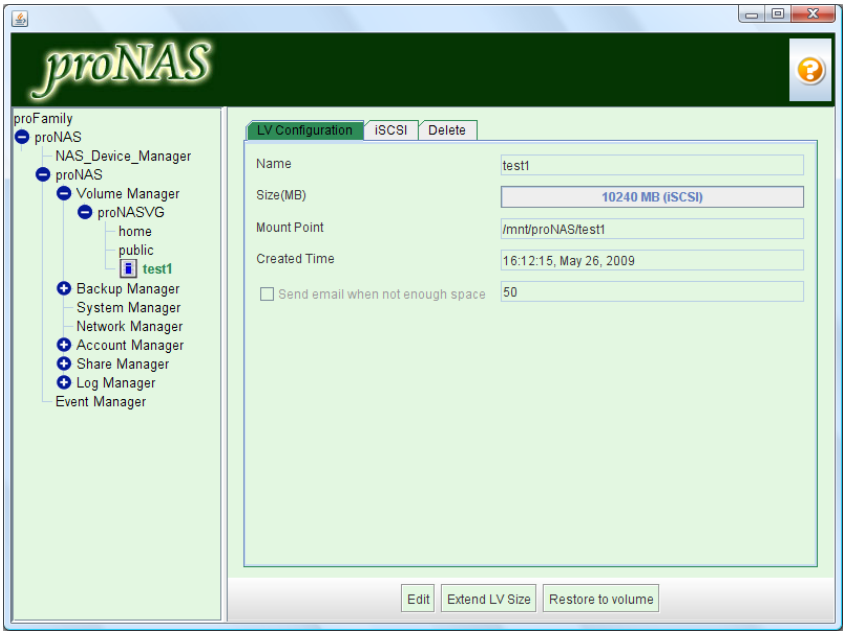
2. Enter the additional capacity for the volume in the Extend size box. Note that you cannot exceed the free/available size from the volume group. Click “OK”.



3. A Confirm message box will be displayed. The iSCSI target will be restarted during volume capacity extension and iSCSI initiator(s) need to re-logon/reconnect. Select “Yes” to continue.



4. The iSCSI logical volume capacity is extended.

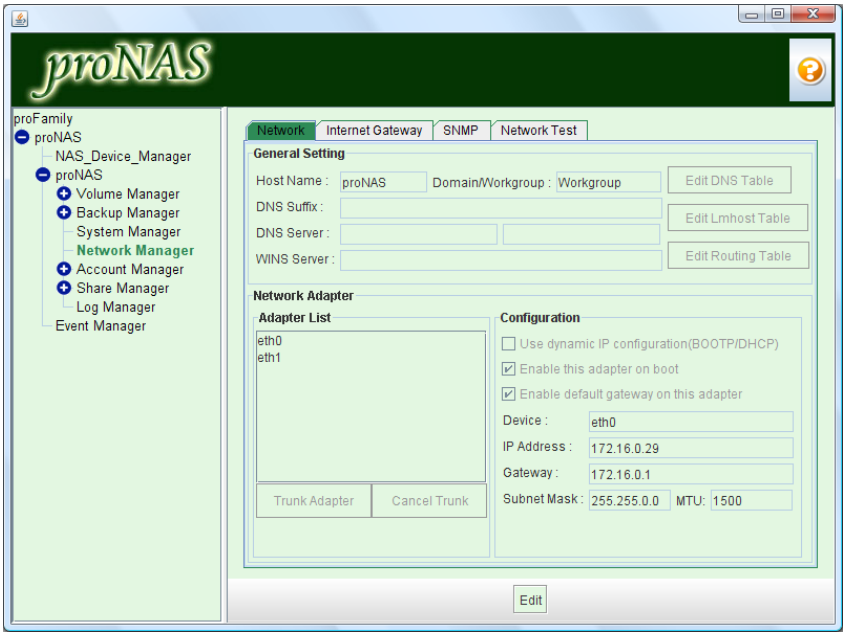


8.2 Network Manager

Using the Network Manager, you can configure the NAS network settings. There are four tabs in Network Manager: Network, Internet Gateway, SNMP, and Network Test.

8.2.1 Network Setting and Trunking

There are two sections in the Network tab, the General Setting section and the Network Adapter section.



The Network tab

Press “Edit” button to configure the Network settings and click “Save” button to update new settings.

General Setting:

- **Host Name -** The NetBIOS name of proNAS, it should be unique.
- **Domain / Workgroup** - Windows domain name or workgroup. Domain name is limited only up to 15 characters. For example: mydomain
- **DNS Suffix** - The DNS suffix appended to server name to complete the server’s FQDN. This includes the domain name, for example: mydomain.local
- **DNS Server** - DNS server is responsible for mapping the machine name and IP Address.
- **WINS Server** - WINS Server is responsible for the setting NetBIOS name resolution.

Edit DNS Table: If you have not set the DNS, you can use this button to edit DNS in the DNS table. This is optional.

Edit Lmhost Table: You can use this option to define the resolution of NetBIOS in the Lmhosts table. This is optional.

Edit Routing Table: You can use this option to define routing table. This is optional.

Network Adapter:

The Network Adapter section consists of the Adapter List and the Configuration section. The Adapter List is the list of available Ethernet ports in the system. The number of ports might be two or three depending on different models.

Adapter List: Lists the available Ethernet adapters.

Configuration:

- **Use Dynamic IP Configuration (BOOTP/DHCP) -** If checked, this specifies that this network connection will dynamically obtain an IP address from a Dynamic Host Configuration Protocol (DHCP) server or from a Bootstrap Protocol (BOOTP) server.
- **Enable this adapter on boot** – If enabled, this adapter will be active when proNAS starts up.
- **Enable default gateway on this adapter** - If checked, the default gateway will be enabled in this adapter. A default gateway is a local IP router that is used to forward packets to destination beyond the local network. Only one default gateway can be enabled in a certain time.
- **Device** - Displays the type of Network Interface Card.
- **IP address** – Shows the current IP address. To edit IP address, enter the new IP address.
- **Gateway** – Shows the current gateway IP address. To edit, type in a new gateway IP address.
- **Subnet mask** – Shows the current subnet mask setting. To edit, type in the new subnet mask number.
- **MTU** – The MTU size (Maximum Transmission Unit) in bytes. To modify the MTU size for this interface, enter the new MTU size.

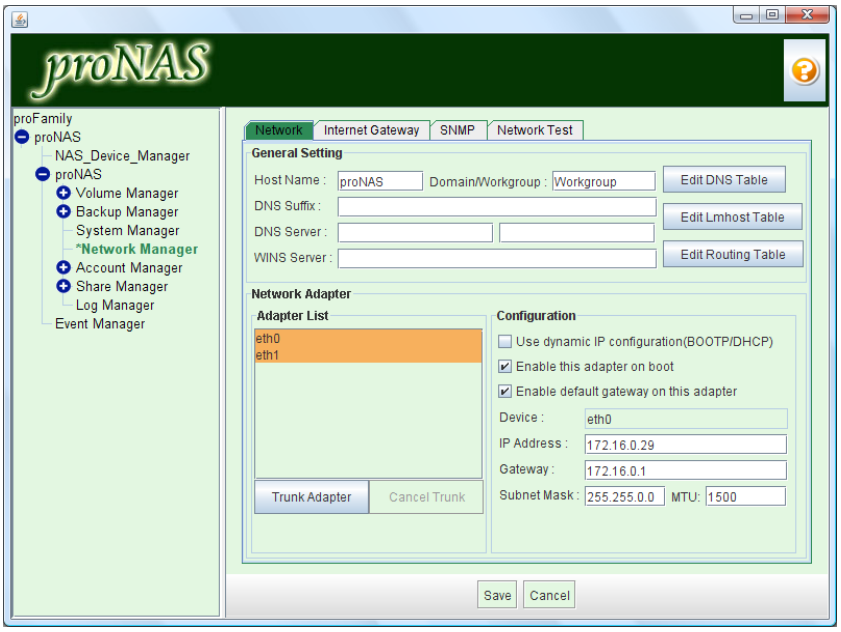
Network Trunking

ProNAS provides the network trunking/bonding function. Ethernet bonding refers to aggregating multiple Ethernet channels together to form a single channel.

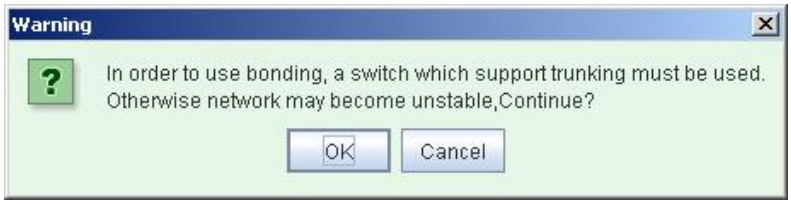
NOTE: It is necessary that the network switch supports the type of trunking mode that will be used. Otherwise, the network connections may become unstable.

To create a trunk adapter:

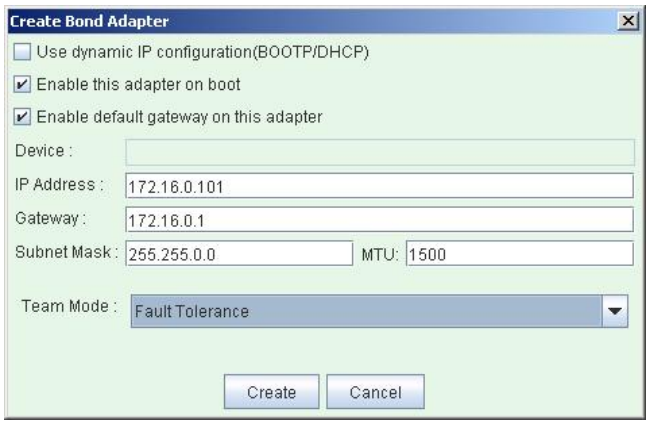
1. Click on the "Edit" button. Press the “Ctrl” key then at the same time select the adapters that will be included in the network trunking then click on "Trunk Adapter" button.



2. A warning message will be displayed. Click “OK” to proceed.


Warning
In order to use bonding, a switch which support trunking must be used.
Otherwise network may become unstable,Continue?
OK
Cancel

3. Setup the network settings. Select the Team Mode to use. Click “Create” when done.



The Team Mode defines the type of operation for the bonded ports.

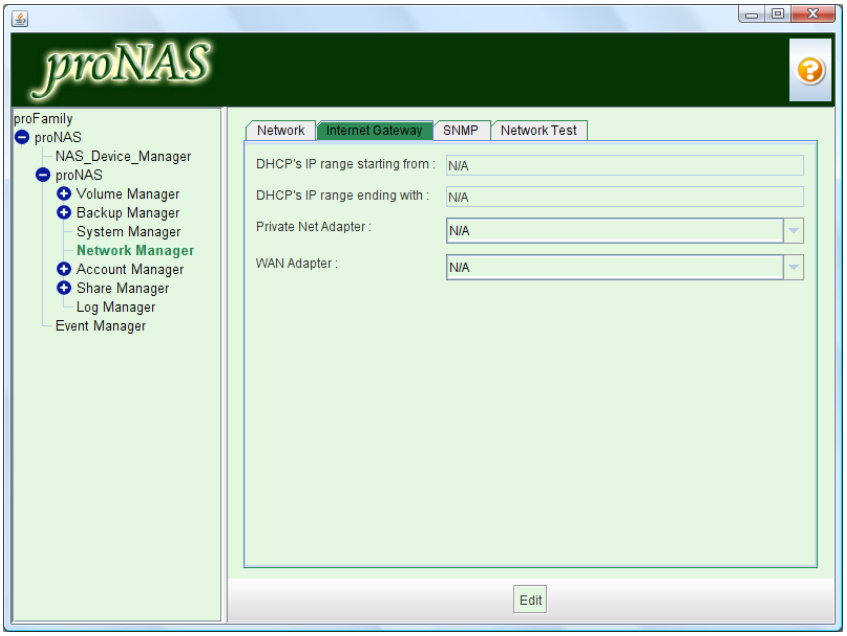
Team Mode options:

- **Fault Tolerant (Active_ Backup)** - Active_Backup policy: If the active Ethernet port fails, the standby Ethernet port will become active. This enhances the availability of access to the NAS.
- **Load balance and Fault Tolerant (XOR)** - XOR policy: Transmit based on source MAC address XOR with destination MAC address. This selects the same slave for each destination MAC address. This mode provides load balance and fault tolerance.
- **Link Aggregation (802.3ad)** - 802.3ad policy: Combines multiple physical network links into a single logical link for increased performance. Transmits and receives on all slaves in the active aggregator. Pre-requisite: the network switch must support IEEE 802.3ad.
- **Load Balance (ALB)** - ALB (Adaptive load balancing) policy: The receive load balancing is achieved by ARP negotiation and does not require special switch support.

4. Connect to proNAS using the new IP address used in network trunking.

8.2.2 Internet Gateway

proNAS provides Internet gateway function which enables proNAS to act as an Internet Gateway, integrating DHCP service, routing and NAT. Using Internet gateway function, administrators can easily enable and disable the Internet access for network users.



To configure Internet Gateway, press “Edit” button.

Configuration options:

DHCP's IP range starting from - means the lower bound (starting) range of private IP addresses for DHCP

DHCP's IP range ending with - means the upper bound (ending) range of private IP addresses for DHCP

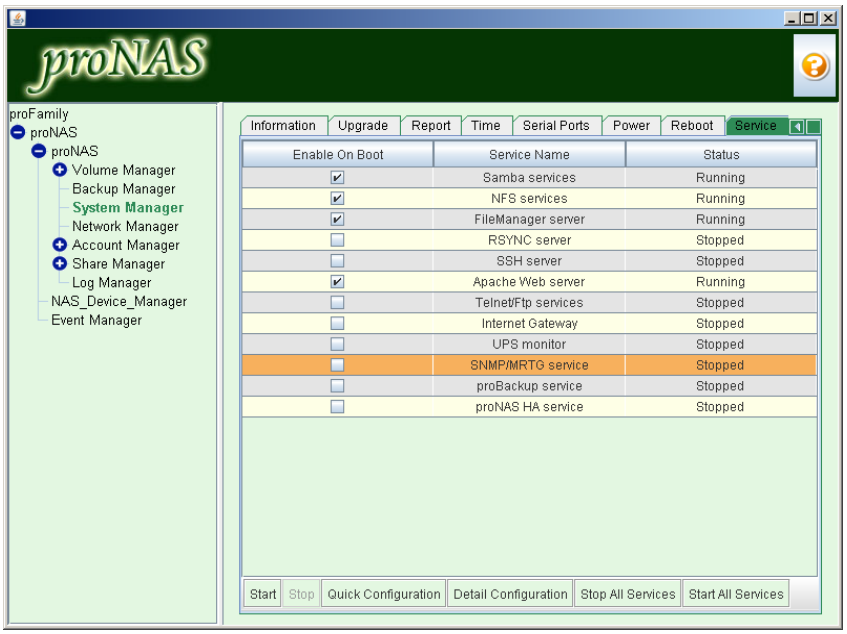
Private Net Adapter - means the port connected to private network. This port has to be a Static port and could also be a Trunk port.

WAN Adapter: means the port connected to WAN or Internet. This port could be a Trunk port.

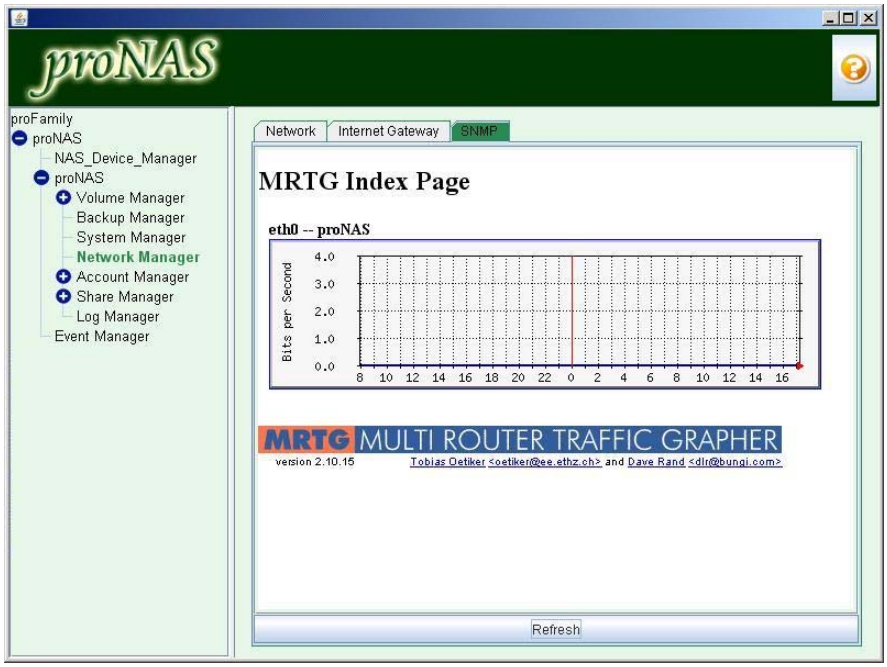
NOTE: When using Internet Gateway function, make sure the Internet Gateway service is enabled in the Service tab of System Manager.

8.2.3 SNMP/MRTG

The SNMP/MRTG service can be enabled to monitor proNAS network traffic. Select Service tab of System Manager then enable SNMP/MRTG service. Click “Start” to enable the service.



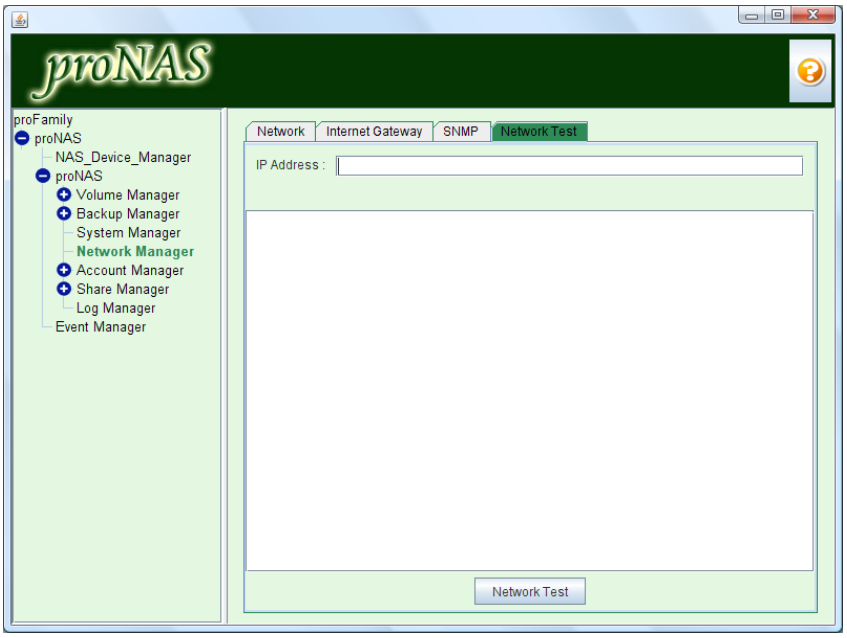
To view the SNMP/MRTG network traffic information, select the SNMP tab in Network Manager.



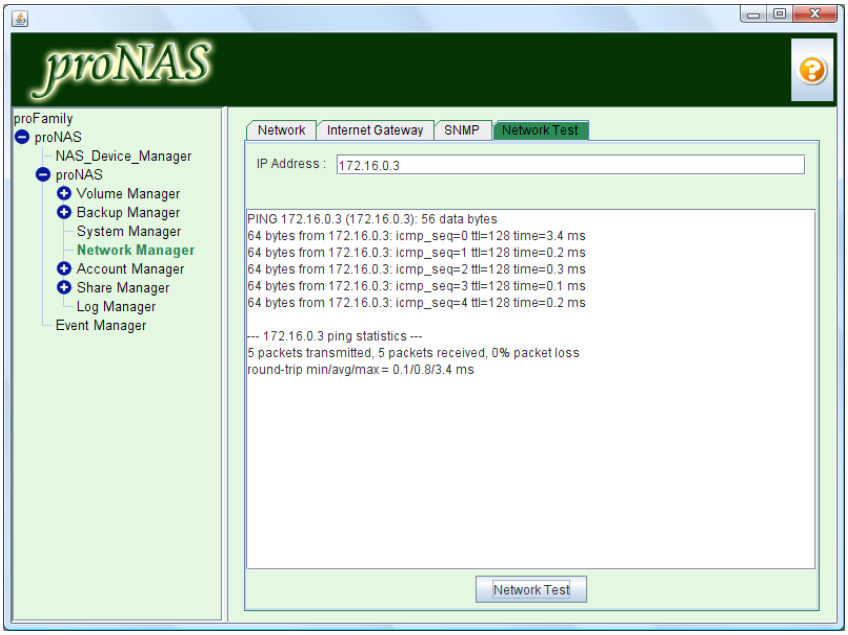
For more information about MRTG service, please visit http://www.mrtg.org.

8.2.4 Network Test

This function allows to test whether a particular host is reachable or to check connectivity to a particular IP address.



To test, enter the IP address in the IP address box then click “Network Test” button. The result will be displayed in the area below the IP address box.



8.3 Account Manager

With Account Manager, the administrator can manage and administer local accounts as well as import external domain accounts. proNAS will utilize external directory services to do account authentications which currently supports ADS/PDC and NIS.

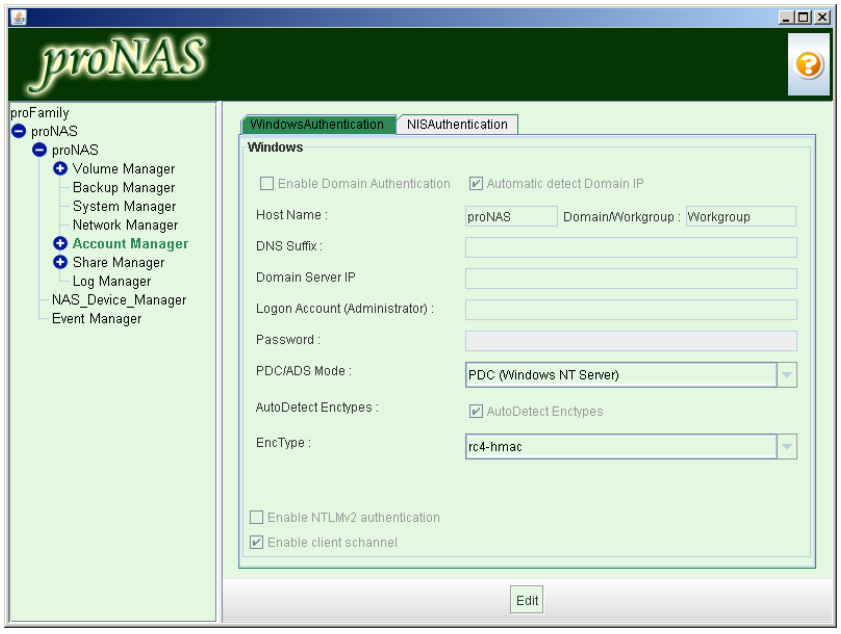
The main functions of the Account Manager are:

- Authentication
- User Account
- Group Management

8.3.1 External Accounts Integration (Joining Windows or NIS Domain)

You can utilize external directory services to authenticate accounts. Currently, PDC/ADS and NIS authentication are supported. You may choose any one of them or both at the same time depending on your network environment.

8.3.1.1 Windows Authentication



If you would like to integrate proNAS with Windows environment, please select “Edit” button then check "Enable Domain authentication". Set the necessary Windows options then click “Save” to update settings.

NOTE: Hostname, Domain name and DNS Suffix need to be set first in Network Manager.

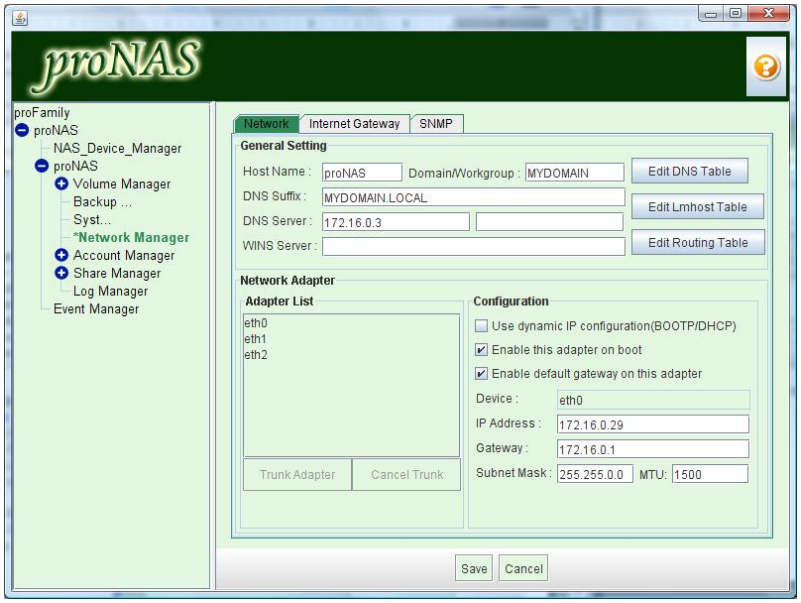
Windows options:

- **Automatic detect Domain IP** – This is enabled by default. When enabled, proNAS will try to automatically detect the domain server's IP address.
- **Hostname** - Indicates the NetBIOS name of proNAS; must be set in Network Manager.
- **Domain / Workgroup** - Windows Domain name; must be specified in Network Manager.
- **DNS Suffix** - The DNS suffix used; must be set in Network Manager.
- **Domain Server IP** - The IP address of the domain server. proNAS will automatically acquire the domain server's IP address after setting the Domain name in Network Manager if "Automatic detect Domain IP" option is enabled. When "Automatic detect Domain IP" option is disabled, you need to manually enter the domain server's IP address.
- **Logon account (Administrator)** – the administrator's logon name in the Domain Controller
- **Password** - the administrator's password in the Domain Controller.
- **PDC / ADS Mode** – The type of Domain Controller. Choose PDC for Windows NT Server or ADS for Windows 2000/2003/2008 Server.
- **Auto Detect Enctypes** – This option automatically detects the encryption type used in Windows authentication. To manually select the encryption type, disable this option and select the preferred encryption type from the EncType drop-down list.
- **Enable NTLMv2 authentication** - This parameter determines whether or not smbclient will attempt to authenticate itself using the NTLMv2 encrypted password. If enable, proNAS will only sent NTLMv2 and LMv2 responses. NTLMv2 authentication protocol is available only on WindowsNT4 with SP4 and Windows 2000 or later. Default is disabled.
- **Enable client schannel** - This controls whether the client offers or even demands the use of the netlogon schannel. Default is auto, means it offers the schannel but does not enforce it.

8.3.1.2 Sample Steps to Join the NAS to Windows AD Domain:

1. Select Network Manager. In Network Manager –> Network tab, click "Edit" to configure network settings.
2. Change the default proNAS Host Name if there are other proNAS systems in the network. Enter the Windows Domain name in "Domain/Workgroup". For example: MYDOMAIN

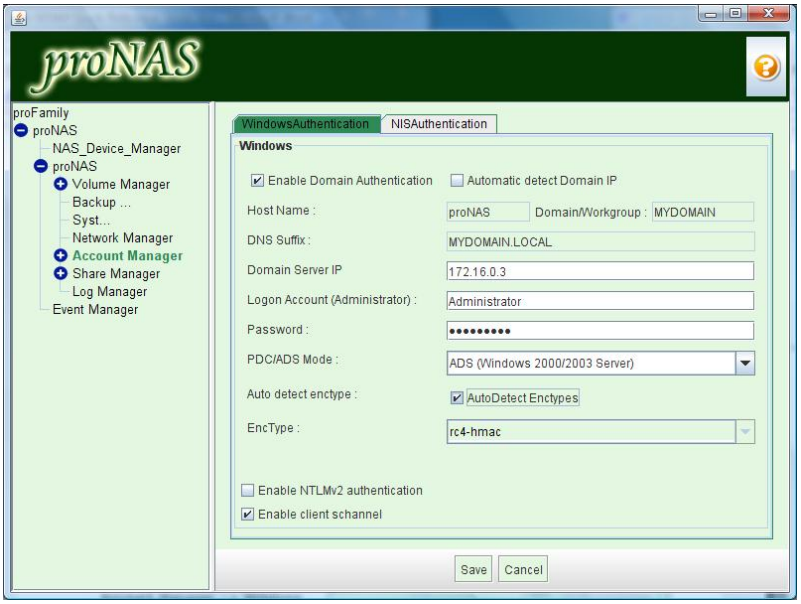
3. Enter the DNS Suffix. The DNS suffix is the name appended to the server name to complete the server's FQDN. This includes the domain name. For example: MYDOMAIN.LOCAL
4. Enter the DNS Server and WINS Server (IP address) as necessary.
5. Click "Save" to update changes.



6. Select Account Manager. In Account Manager –> Windows Authentication, click "Edit".
7. Tick "Enable Domain Authentication" option.
8. If the Domain Server IP is not detected (not shown), you can manually specify the Domain Server IP by removing the check mark in "Automatic Detect Domain IP" and entering the Domain Server IP address.
9. Enter the Domain Administrator Account and Password.

NOTE: No need to include "domain-name\" in Domain Administrator Account.

10. Select the Domain Server mode (PDC or ADS).
11. If needed, change the encryption type to the same type used by your domain server.
12. Click "Save". The NAS will be joined to Windows Domain in a while.



13. To verify, select Account under Account Manager; the user accounts should be shown. You can also verify group accounts in Group List.

8.3.1.3 NIS Authentication

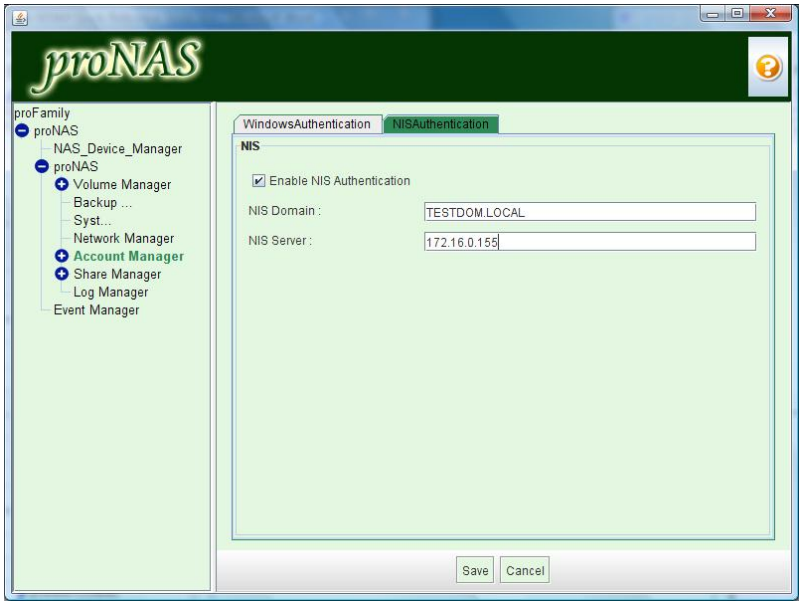
If you would like to integrate proNAS with UNIX/Linux environment, please select “NIS Authentication” tab and click “Edit” button then check "Enable NIS authentication". Set the necessary configuration options then click “Save” to update settings.

Configuration Options:

- **NIS Domain** - Enter the NIS domain name
- **NIS server** - Enter the IP Address of NIS server.

8.3.1.4 Sample Steps to Join NIS Domain:

1. Under Account Manager, select NIS Authentication tab. Click Edit.
2. Check the Enable NIS Authentication option. Enter the NIS Domain name (e.g.: TESTDOM.LOCAL) and NIS Server IP address or FQDN. Click Save when done.
3. Click Account under Account Manager to verify that the NIS Accounts are listed in the Account List, or select Group to display the NIS Groups in the Group List.



8.3.2 Local Account and Group Management

Account Management

The Account List in Account Manager includes Local users and External users, ADS/PDC or NIS.

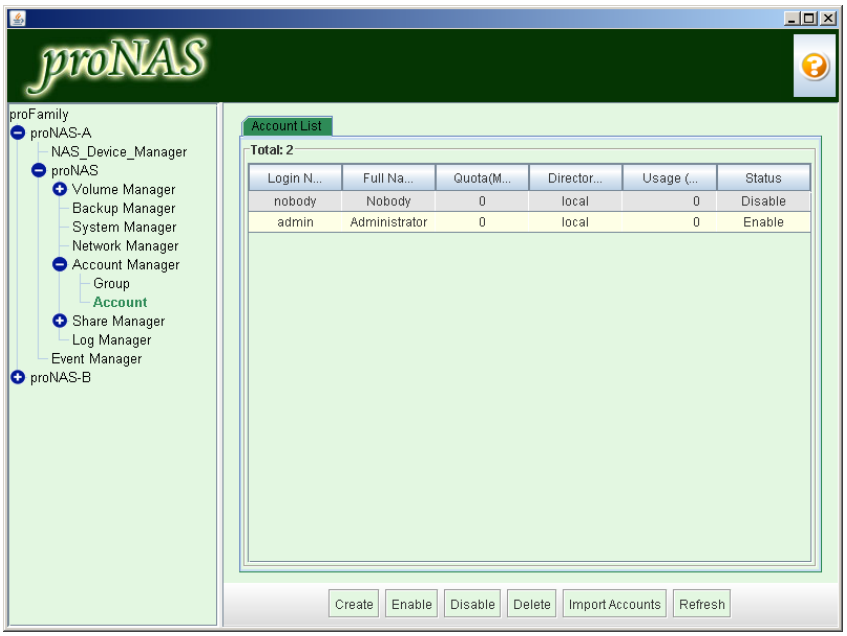
In Account menu, admin can perform the following functions:

- Create a new Local Account
- Enable and Disable an Account
- Modify and Delete an Account
- Mass Import Accounts
- Refresh the Account List

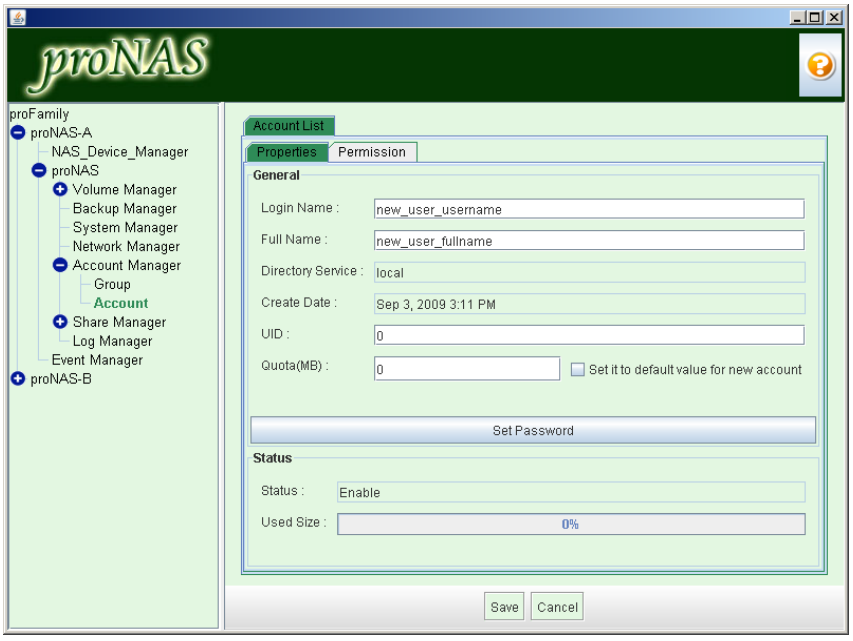
Creating a new Local account

Following are the steps to create a new Local account:

1. Select Account Manager in the proFamily tree. Choose Account node under the Account Manager. It will display all accounts under the Account List tab.



2. Press the "Create" button. System will display "Account List tab". Account List tab consist of two tabs, "Properties" and "Permission". In the Properties tab, enter the necessary information.



General:

- **Login Name** - Input the login name, it should be unique in proNAS
- **Full Name -** the complete name of the account
- **Directory Service -** system will display if the directory service is Local or ADS/PDC,NIS
- **Create Date -** system will display the create date of the account.
- **UID -** In UNIX or Linux, OS will assign a unique user number called UID to access the system resource. (UID range is 1 to 65535). proNAS may either assign a new UID automatically starting from 500 or you can manually specify the UID. Domain accounts will have a UID starting from 10000-30000.
- **Quota Size (MB)** - This specifies the quota (usable space) of a user for its home folder. The default is 0, which means user has unlimited home folder quota. The limit then is the size of the home volume.
- **Set it to default value for new account** – When this option is enabled and the Quota Size value has been changed from 0 to another value, the new value set in Quota Size will become the new default Quota Size when other accounts are created.
- **Set Password** – Click this button to set the account's password. Passwords have to be at least 6 characters.

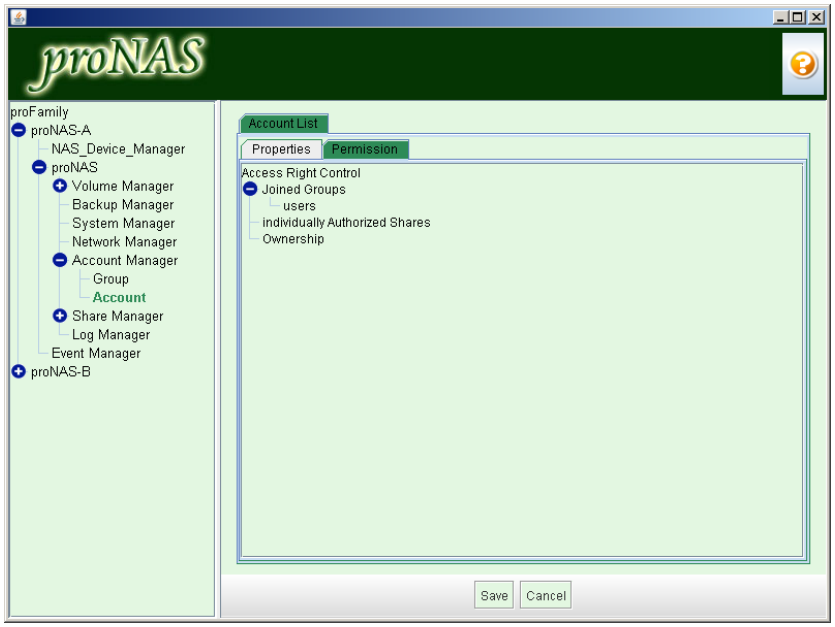
Status:

- **Current status:** Displays Enable or Disable.
- **Used Size (MB):** Displays the current used size.

Use the following guidelines to ensure that you are using a valid Account name:

- Account names must start with a small alphabet letter.
- Account names cannot be longer than 32 characters.
- Account names should be unique. No account names must be the same. No account names must be the same with share names.
- Account names cannot contain blank spaces.
- Account names cannot begin with a dash (-) and cannot consist of only a single dash.
- Account names cannot contain the following characters: /\[]";:|<>+=,?*
- Account names cannot be duplicated with the system default accounts, i.e. root, mail, news, operator, gopher, nobody, ftp, games, rpc, adm, nobody, etc.

3. After completing the settings, press the "Save" button to save settings, or you may go to "Permission" tab to have a look at the permissions of the account then click “Save” button when done.



Permission tab

- **Joined Groups:** The account has gained access right because of joining certain groups.
- **Individually Authorized Shares:** Implies that the account has gained access rights individually.
- **Ownership:** Implies that the account has gained access right because it is the owner.

NOTE: Newly created accounts will automatically be a member of "users" group.

Enabling and Disabling an Account

Account Manager allows the administrator to enable or disable a user account. When an account is disabled, the account cannot be used to login and access proNAS.
To forbid certain user account in accessing proNAS, highlight the account then press "Disable" button. The account will be shown with “Status” as Disable. If you would like to re-enable the user account proNAS, press "Enable" button. Disabling account "admin" is not allowed as well as all ADS/PDC and NIS accounts.

Deleting an Account

If you would like to delete a certain account, highlight the account then press "Delete" button. The user's home directory will be deleted. If the user owns one of the share, the owner of that share will be set to "admin". Account "admin" is not allowed to be deleted as well as ADS/PDC and NIS accounts.

Modifying an Account

If you want to modify an account, double-click on the account. You can only modify the password and permissions. If the account is an external domain account (created by ADS/PDC or NIS domain server), the account and password can not be modified in proNAS Account Manager. In such a case, you can only modify the permissions.

Importing of Accounts

proNAS provides Import Account function for creating large number of accounts instead of adding an account one by one. Administrator can create multiple user accounts in a text file with the following format: UID, Logon Account, Logon Password, Full Name. Example:

1019, david, proware, David Huang

1020, rocky, proware, Rocky Lee

To import the accounts, click on "Import Accounts" button then select the text file.

NOTE: The information for each account must start on a new line. If account creation fails for any account, proNAS skips that line (of account information) and continues with the next line.

Refreshing the Account List

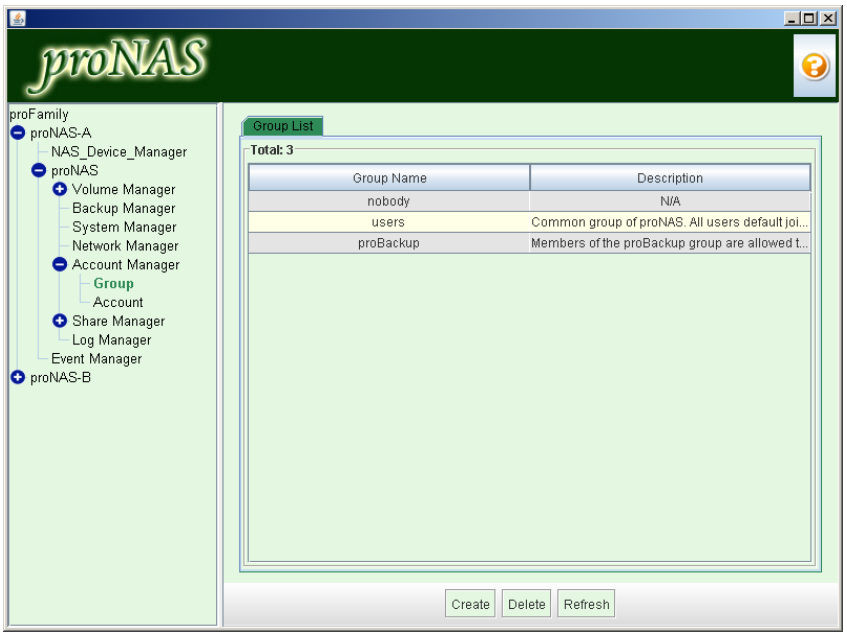
Use the “Refresh” button to automatically synchronize any new accounts created in ADS/PDC or NIS domain.

Group Management

Using group management, admin can organize access to proNAS shares. For example, a Sales group can be created for the sales department and this group can be assigned read-write access to the Sales Report share. All account members of the Sales group can have access to the Sales Report share.

Group List tab

The Group List tab shows the Local and External (ADS/PDC or NIS) Groups.



Group management allows the administrator to:

- Create or Delete a Local group
- Modify a Group
- Refresh the Group List

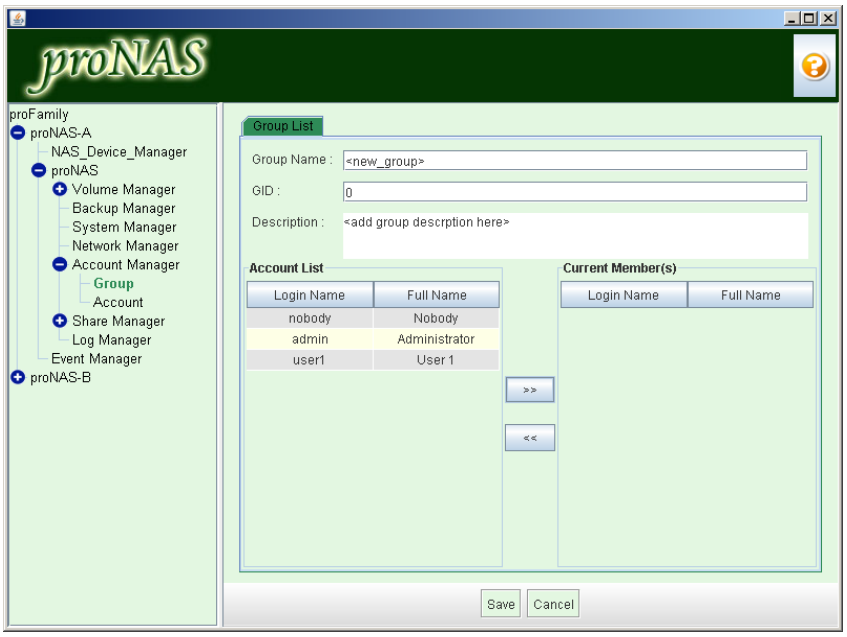
proNAS has two default groups, "users" and "proBackup". Every local user that will be created will automatically become a member of users group. proBackup group is used by proNAS for the proBackup service.

Creating a new Local Group

When a Local Group is added, it is created in the local account database of NAS. One account can become a member of more than one group.

Following are the steps to create a new Local Group:

1. Select Account Manager in the proFamily tree. Choose Group node under the Account Manager. It will display all groups under the Group List tab. Press the "Create" button.
2. Enter the necessary information. Refer to options below.



Create Group Options:

- **Group Name** - Enter the name of new group. It should be unique.
- **GID** - Group ID. proNAS will either automatically assign a GID when you create a group, or you can manually specify a GID.
- **Description** – Additional information or description about the Group can be entered here.

Account List – shows the list if accounts that are available and can be joined to the group

Current Member(s) – shows the list if accounts that are currently member of the group

NOTE: AD domain accounts cannot be joined to local groups.

Use the following guidelines to ensure that you are using a valid Group name:

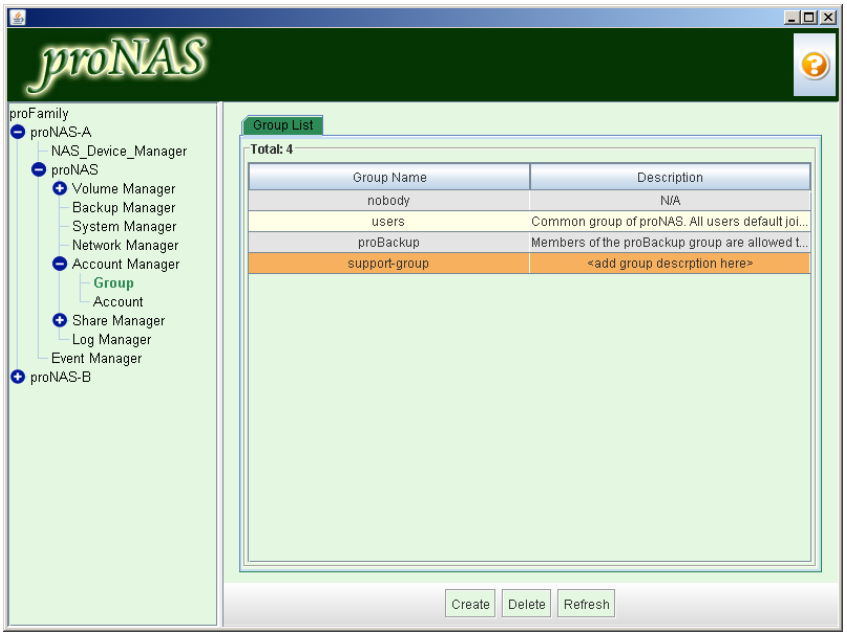
- Group names cannot be longer than 16 characters.
- Group names should be unique. No group names must be the same.
- Group names cannot contain blank spaces.
- Group names cannot begin with a dash (-) and cannot consist of only a single dash.

- Group names cannot contain the following characters: /\[]";:|<>+=,?*
- Group names cannot be duplicated with the system default groups, i.e. root, mail, news, operator, gopher, nobody, ftp, games, rpc, adm, nobody, etc.

3. In the Account List, select the account(s) that will be joined to the group then click the “>>” button. The accounts will appear in the Current Member(s) list. To remove an account from the group, select the account in Current Member(s) list then click “<<” button.
4. Click “Save” button to save settings.

Deleting a Local Group

To delete a group, select the group to be deleted and then click the "Delete" button. ADS/PDC and NIS groups are not allowed to be deleted. Default group "users" and "proBackup" cannot also be deleted.



Modifying a Group

To modify a group, double click the group in Group List tab. The "Group List" tab will be displayed in edit mode. Group name, description, group members are allowed to be modified however this is only applicable to local groups. ADS/PDC and NIS groups are not allowed to be modified. Default group "users" and "proBackup" cannot be modified. ADS/PDC and NIS domain accounts are also not allowed to be joined to any local group except to "proBackup" group.

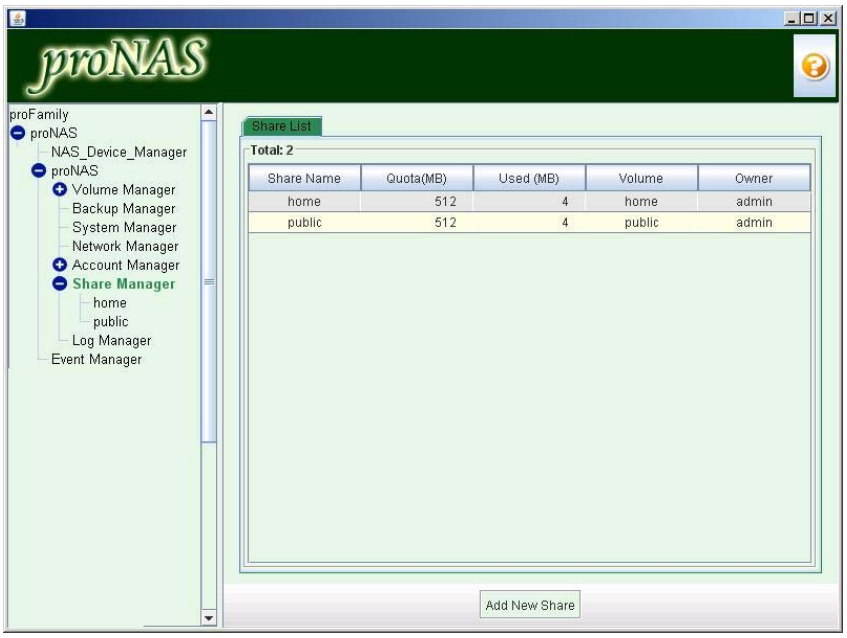
Refreshing the Group List

Use the “Refresh” button to automatically synchronize any new groups created in ADS/PDC or NIS domain.

8.4 Share Manager

In proNAS Share Manager, you can create and configure a Share, assign a share owner, assign user permission, and specify file sharing protocol. Under this node you can also use duplication function and rsync utility. Duplication is a share function in which you can replicate your share into another share using file level replication. Rsync utility is used to copy files either to or from a remote host, or locally on the current host.

In the "Share List" tab, you can list the current shares and also display share information such as share name, quota, used space, logical volume and share owner. There are 2 Default Share in proNAS: "home" and "public".



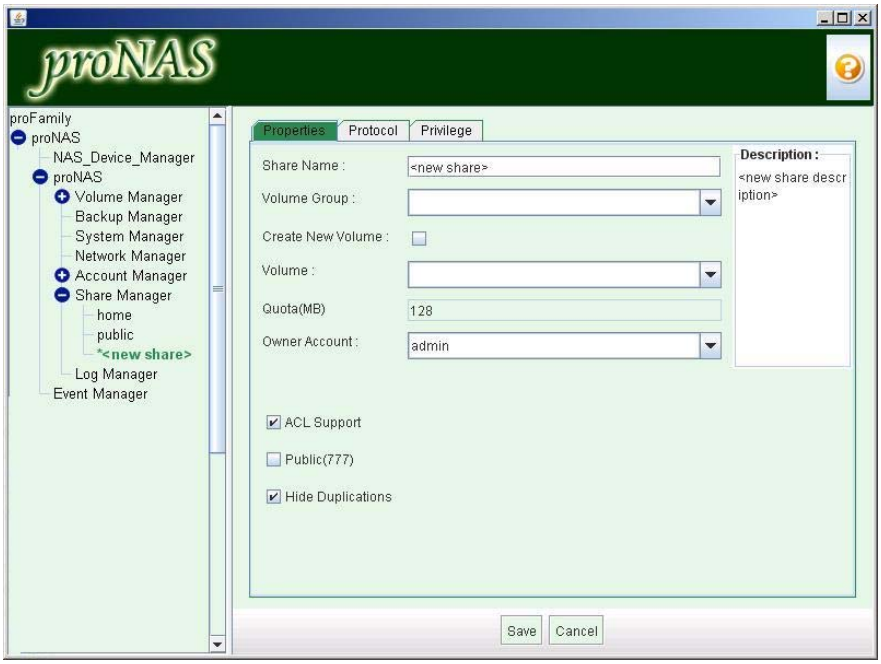
Share folder gets created under a logical volume. Make sure that an LV is already created before creating the share folder or admin can create the share folder and LV simultaneously, which can be done using the option “Create New Volume” in Properties tab of Share Manager.

8.4.1 Share Management

8.4.1.1 Creating a New Share

To create a new share folder:

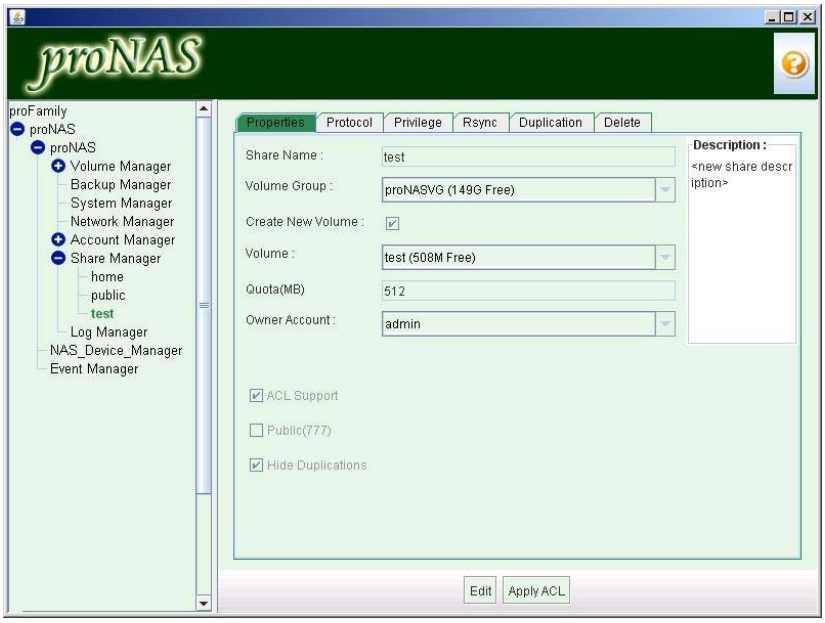
1. Select Share Manager then press "Add New Share" button.
2. Configure all necessary share options in Properties, Protocol, and Privilege tabs. Refer to Properties Setting, Protocol Setting, and Privilege Setting Sections in the succeeding pages.
3. Click “Save” button to save share settings.



NOTE: After creating the share and setting the Properties, Protocol and Privilege tabs, you can go back to these tabs and modify the various options. To edit, click the share name in Share Manager and click “Edit” button.

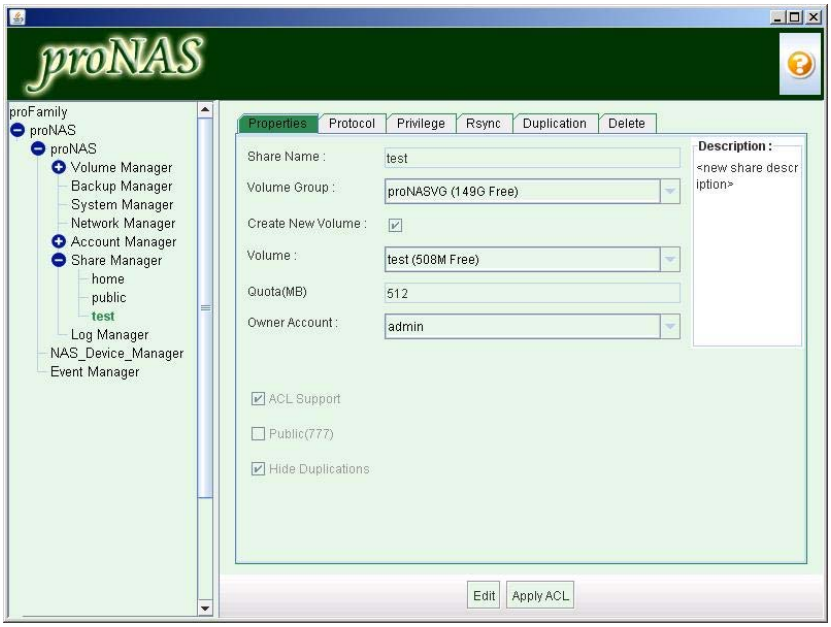
8.4.1.2 Applying ACL

When applying ACL in a share, all the files and subfolders under this share will inherit the share's permission. "Apply ACL" will propagate the ACL settings of the share folder into all of its child directories and files. For example, if user1 has read/write permission on the sub-folder but read only on the share, after applying ACL, user1 will now have a read-only permission on the sub-folder.



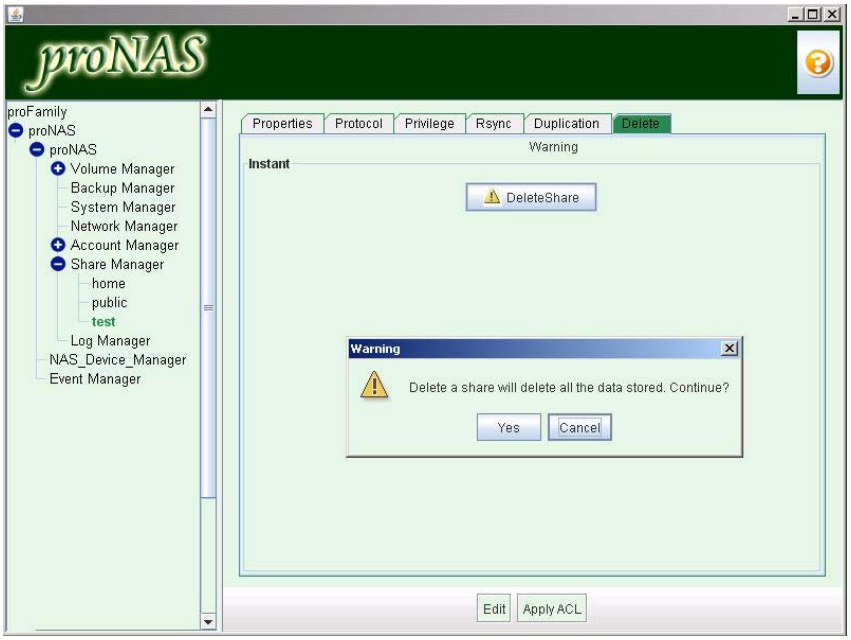
8.4.1.3 Modifying a Share

After creating the share, you can modify the Properties, Protocol, and Privilege tabs, as well as setup the Rsync and Duplication functions. Click the “Edit” button to modify the share.



8.4.1.4 Deleting a Share

If you delete a share, all the data in the share is deleted. If the data in the share is no longer needed or a backup of the data has been made, you may delete a share. If there is no data backup, we recommend you to create a backup first before deleting a share.



8.4.2 Properties Setting

The Properties tab contains the following settings:

- **Share Name -** Input the share name, it should be unique in proNAS.

  Use the following guidelines to ensure that you are using a valid Share name:

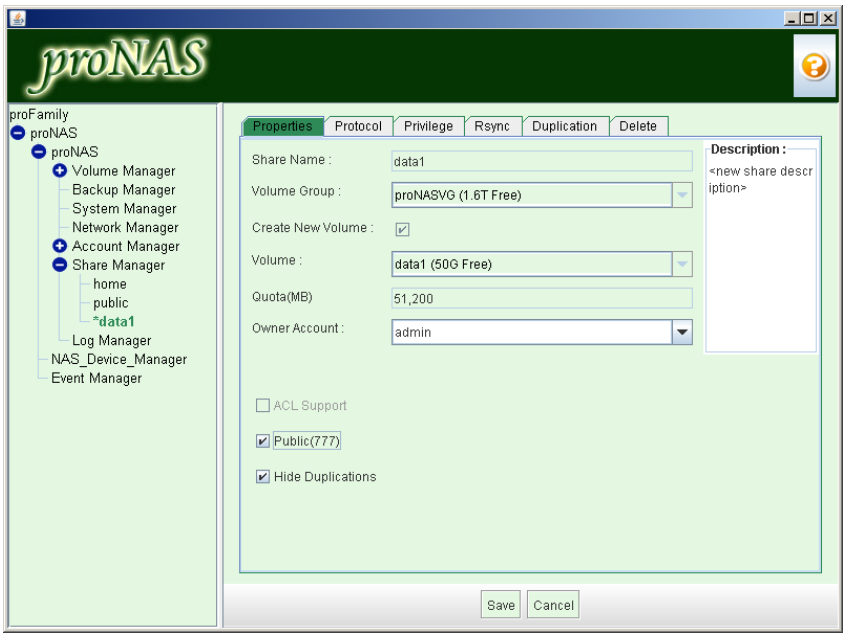
  - Names cannot be longer than 31 characters.
  - Names should be unique. It cannot be a duplicate with other LV names, shares, and Account names.
  - Names cannot contain blank spaces.
  - Names cannot begin with a dash (-) and cannot consist of only a single dash.
  - Names cannot contain the following characters: /\[]";:|<>+=,?*

- **Volume Group (VG)** - Choose a volume group from the list. Only Volume groups that has member disk will be displayed. System will also display the available space of the volume group.
- **Create New Volume (LV)** -If you check this option, system will create LV as well as create the new Share. The LV name will be the same as the share name.
- **Volume -** Select a logical volume from the selected volume group.
- **Quota (MB) -** Input the size of the share. This is also the size of the logical volume to be created if you choose to create a volume at the same time.
- **Owner Account -** Specifies the owner of the share.
- **ACL Support** – Specifies if the share will support ACL permission (option is enabled by default) or support “chmod” permission.
- **Public (777)** - This option allows you to set a share as a public share. When enabled, any user within the specified private net can connect to this share.
- **Hide Duplications** - This option allows you hide or unhide the "_Duplication" folder in this share. The default will be hidden.

8.4.2.1 Steps to Make a Share Folder a Public Folder Accessible to All Users:

NOTE: It is not recommended to set a Share as a Public Share folder. Any local NAS account or Windows/NIS domain account (if NAS is joined to the domain) can login to the share with Read/Write privilege.

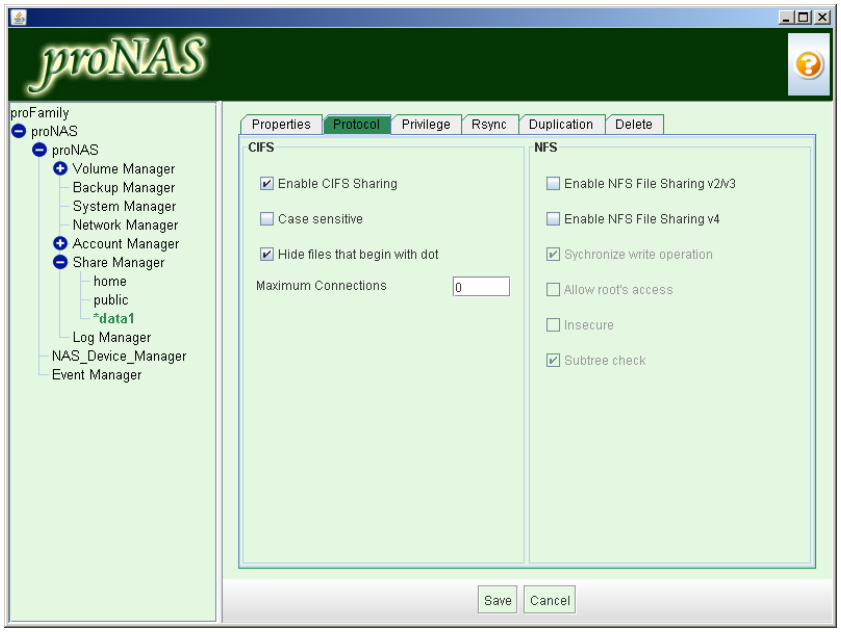
1. Select Share Manager. Select the share name that will be made accessible to all users.
2. In the Properties tab, click “Edit”. Select (tick) the “Public (777)” option.
3. Click “Save”. When a warning message is displayed, click “OK” to proceed.



NOTE: If you need to reassign ACL, click “Edit” then enable (check) the “ACL Support” option. The “Public (777)” option will be automatically disabled (unchecked).

8.4.3 Protocol Setting

ProNAS supports the following share protocols: CIFS and NFS, which can be set in Protocol tab when creating the share or when in edit mode.



8.4.3.1 CIFS

- **Enable CIFS Sharing** - This option is used to enable or disable CIFS sharing. By default, this option is enabled. Windows clients usually use CIFS to connect to this share. Note that newer versions of Mac OS X also support CIFS share connection without using AppleTalk.
- **Case sensitive** - This control whether filenames are case sensitive.
- **Hide files that begins with dot** - This option controls whether files starting with a dot will appear as hidden files.
- **Maximum Connections** - This option limits the number of simultaneous connections at a certain time. Default value is zero, which means an unlimited number of connections are possible in this share.

NOTE: The default setting of "Maximum Connections" is 0. If there is a need to limit the number of simultaneous connections to a CIFS share, set it to specific number instead of 0.

8.4.3.2 NFS

- **Enable NFS file sharing v2/v3** - This specifies whether to enable or disable NFS version 2 / version 3 file sharing. NFS is used in UNIX/Linux environment.
- **Enable NFS file sharing v4** - This specifies whether to enable or disable NFS version 4 file sharing.
- **Synchronize write operation** – Use this option to enable or disable write caching
- **Allow root's access** – Use this option to allow or disallow access by root super user account
- **Insecure** - If you choose this option, it means only the port under 1024 can access, it provides higher security
- **Subtree check** – Use this option to enable or disable subtree checking. A subtree check happens if a subdirectory of a filesystem is exported, but the whole filesystem isn't then whenever a NFS request arrives, the server must check not only that the accessed file is in the appropriate filesystem (which is easy) but also that it is in the exported tree (which is harder).

Accessing proNAS shares under Linux

For NFS share:

Usage: mount -t nfs x.x.x.x:/mnt/proNAS/volume/share /mnt/temp
Where:

x.x.x.x = proNAS IP address
/mnt/proNAS/volume/share = the complete path of the NFS share. You may use the command "showmount -e x.x.x.x" to query the complete path.
/mnt/temp = local mount point on the client

For CIFS share:

Usage: mount -t smbfs //x.x.x.x/share /mnt/temp -o username=account,password=secret
or
mount.cifs //x.x.x.x/share /mnt/temp -o username=account,password=secret
or
smbmount //x.x.x.x/share /mnt/temp -o username=account,password=secret

where:

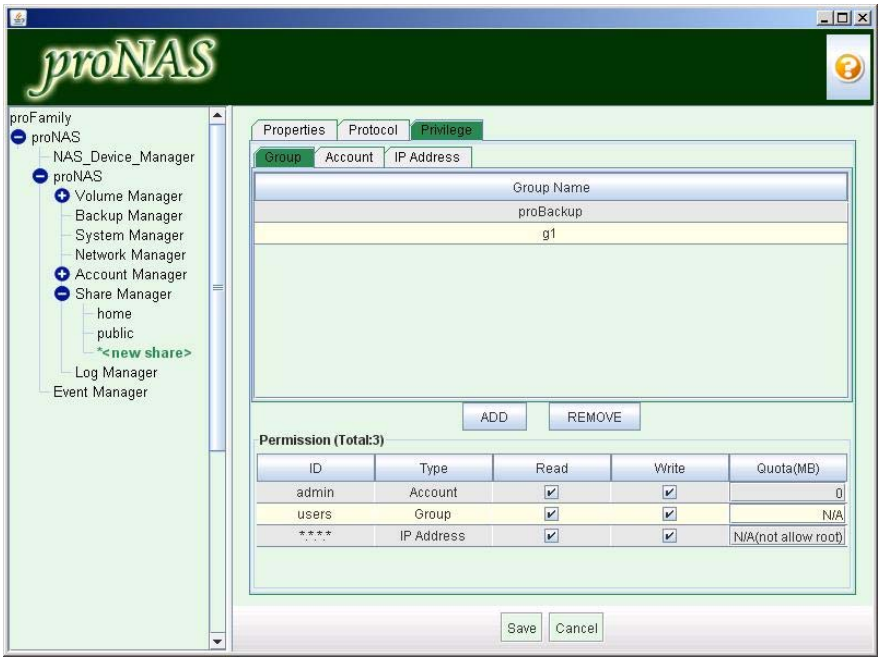
x.x.x.x = proNAS IP address
share = CIFS share name. You may use the command "smbclient -L x.x.x.x" to query the CIFS share names.
/mnt/temp = local client mount point.
-o username=account,password=secret = the account name and password

8.4.4 Privilege Setting (Permission)

Using Privilege tab, administrator can set the ACL (Access Control List) for share folder either by Group, Account, or IP Address.

8.4.4.1 Group

You can assign specific group read or read/write permission for certain share folder. Choose the group and press "ADD" button. The group will displayed in the permission list, and check "Read" or "Write" or check both and press "Save". If you would like to remove the group with ACL setting to certain share folder, select the group name and press "REMOVE" button.



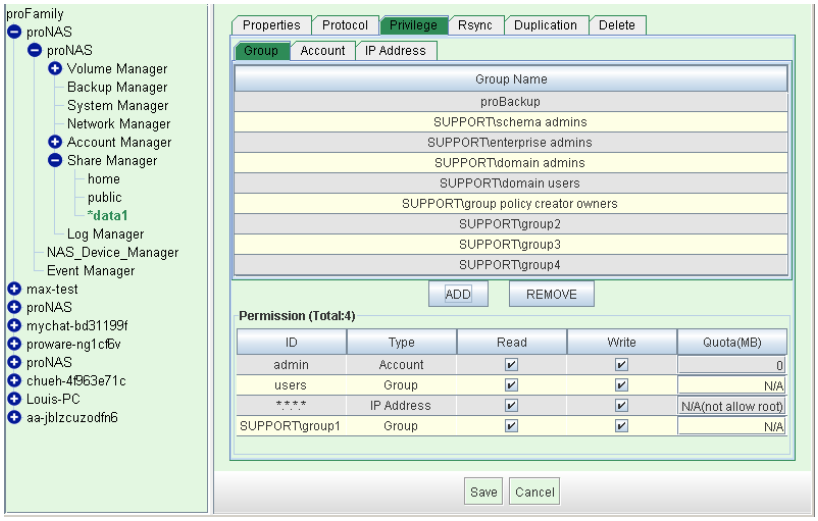
Sample Steps to Assign Group Account Permission to Share:

1. Select Share Manager. Select the share name where account will be given permission, and click Privilege tab.
2. Click “Edit”. Select Group tab.
3. Select the group account that will be given permission and click “ADD”.

NOTE: When group account name is selected, it will be highlighted. If you want to select more than one group account at the same time, press “Shift” key then click the groups you want to add to Permission list.

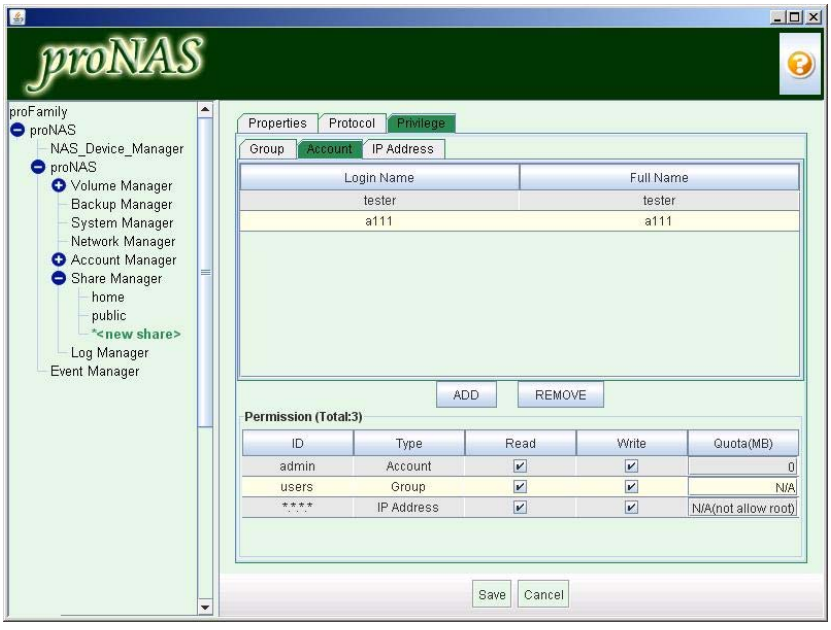
4. In the Permission list, modify the permission, either Read-Only (no check mark in “Write” box) or Read/Write (both “Read” and “Write” boxes have check marks).

5. Click Save.



8.4.4.2 Account

You can assign specific account user read or read/write permission for certain share folder. When you set the account with ACL, it may be necessary to remove the users group from the permission list in order to prevent access of other members of “users” group to the share. Choose the account and press "ADD" button, and the account will be displayed in the permission list. Check "Read" or "Write" or check both and press "SAVE".



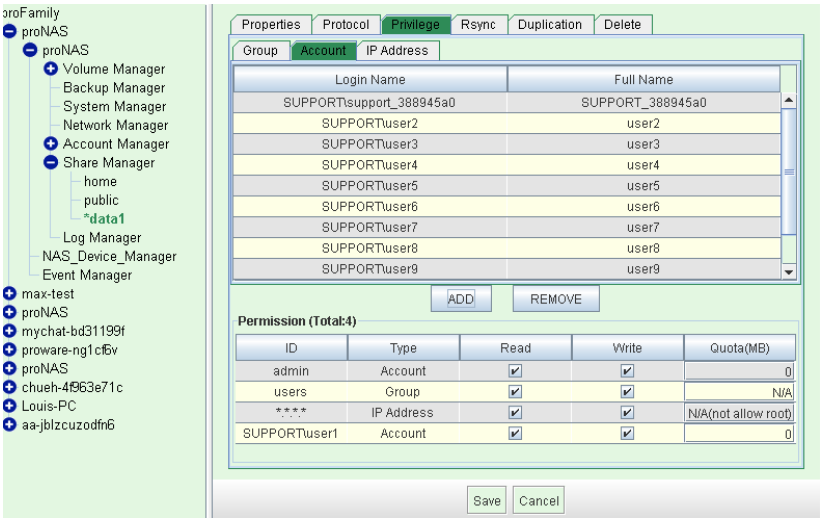
NOTE: Newly added users or groups may have no permissions on the existing files or sub-folders until "Apply ACL" button is executed.

Sample Steps to Assign User Account Permission to Share:

1. Select Share Manager. Select the share name where account will be giver permission, and click Privilege tab.
2. Click “Edit”. Select Account tab.
3. Select the account name that will be given permission and click “ADD”.

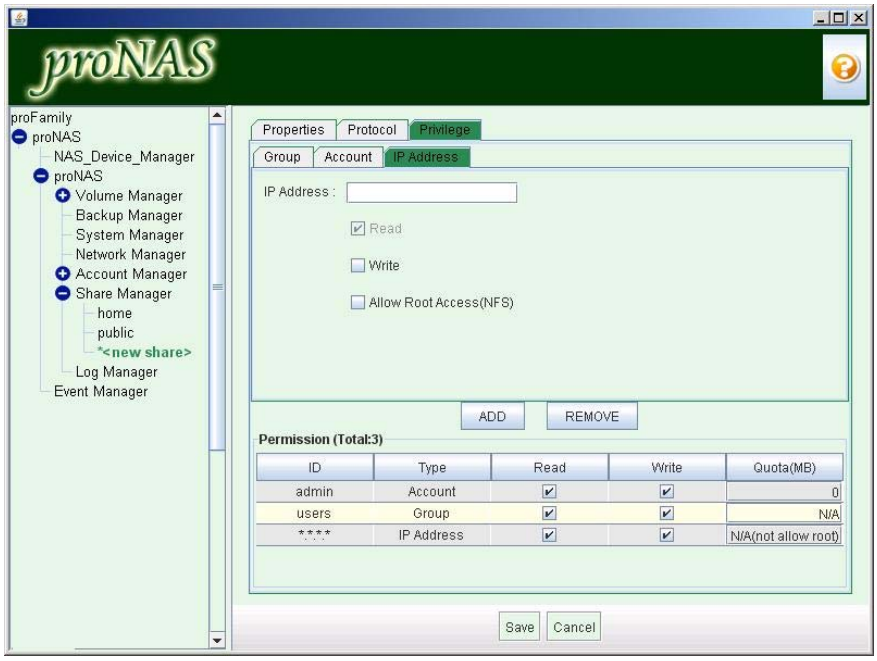
NOTE: When account name is selected, it will be highlighted. If you want to select more than one account at the same time, press “Shift” key then click the accounts you want to add to Permission list.

4. In the Permission list, modify the permission, either Read-Only (no check mark in “Write” box) or Read/Write (both “Read” and “Write” boxes have check marks).
5. Click Save.



8.4.4.3 IP Address

This option allows you to set a certain range of hosts to have an access into proNAS. By default, the IP address is set to *.*.*.* which means that it will accept connections from any host. If set to 192.168.100.*, this will only allow connections from your private network 192.168.100 and all other connections will be refused.



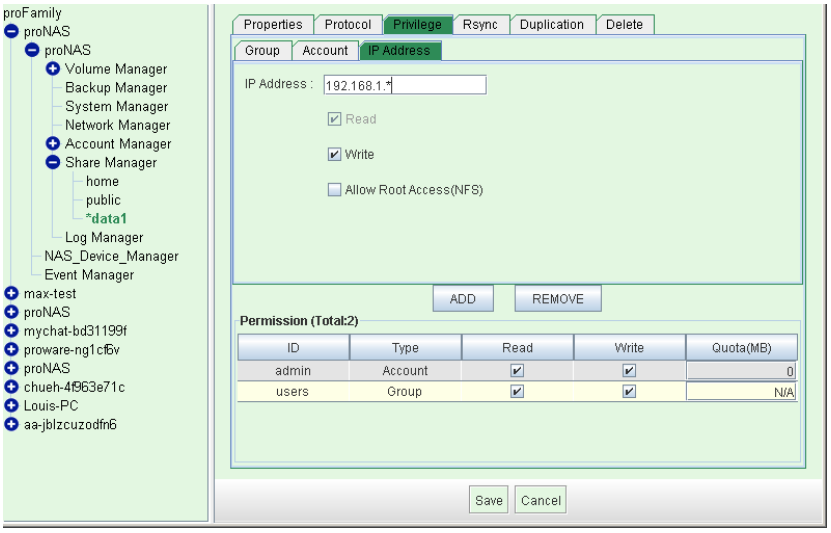
NOTE: Not all ACL permission settings may be applicable to all share protocols. If you set NFS protocol, it can support all ACL setting mentioned above. If you set CIFS protocol, read only IP address will not be honored.

Sample Steps to Limit Share Connections to Selected IP Range:

1. Select Share Manager. Select the share name where account will be giver permission, and click Privilege tab.
2. Click “Edit”. Select IP Address tab.

NOTE: BY default, all IP addresses (*.*.*.*) have Read / Write access to the NAS. If you restrict NAS connections from specific IP range, only the selected IP range can access the NAS share. Group Permission or User Account Permission is still needed to be assigned in order for users to gain access to the share folder.

3. To remove *.*.*.*, select “*.*.*.*” from Permission list and click “REMOVE”.
4. To add an IP range, enter the IP range (e.g.: 192.168.1.*) in the “IP Address” box, check the “Write” box to assign Read-Write access if necessary, and click “ADD”.
5. Click “Save” when done.



Permissions:

This section lists the permissions that you can assign for each user, group, or IP address. When you create a share, the default owner which is the "admin" will be granted full control. The same is also true for "users" group and the "*.*.*.*" for IP address.

Listed below are the share permissions defined in proNAS:

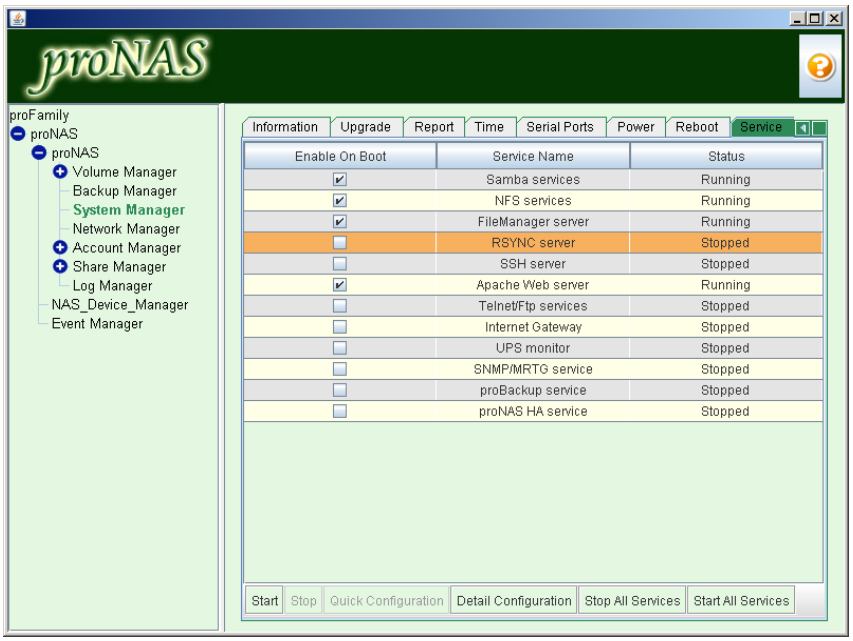
Read Only			**Read+Write**		
	Allow	Deny		Allow	Deny
Access share, sub-folder	☑		Access share, sub-folder	☑	
Read	☑		Read	☑	
Write		☑	Write	☑	
Edit/Modify		☑	Edit/Modify	☑	
Delete		☑	Delete	☑	
Rename		☑	Rename	☑	

Setting the amount of quota to a specific user

In the "Quota(MB)" field, you can input the quota of an account which is granted permission to the share. Press the "Enter" key after you input the amount in Quota(MB) field. To remove the quota limit, set the Quota(MB) to 0 then press "Enter" key.

8.4.5 Rsync

Rsync copies files either to or from a remote host, or locally on the current host. It is also a utility that provides fast incremental file transfer. proNAS Rsync implementation can be set either in server mode or client mode. Server mode means that proNAS can accept incoming Rsync connections, where as in client mode, proNAS is the one who initiates the synchronization. To use as a server mode, you must start the "RSYNC server" first. Go to System Manager -> Service tab, highlight "RSYNC server" then click the "Start" button.



Some of the additional features of Rsync are:

- Support for copying links, devices, owners, groups, and permissions.
- Pipelining of file transfers to minimize latency costs
- Support for anonymous or authenticated Rsync daemons

Server Mode:

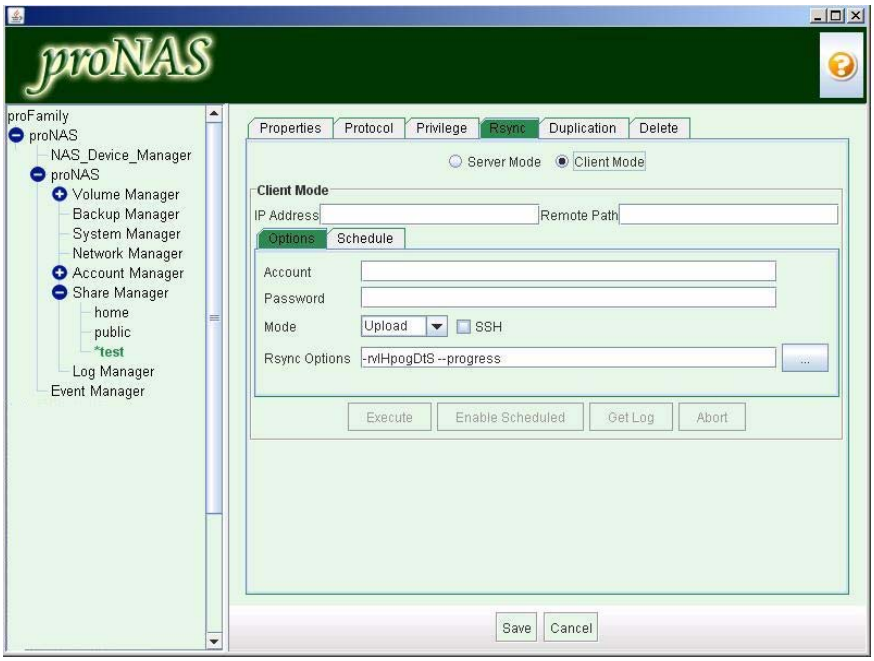
When proNAS system is in Server Mode, the Rsync clients can connect either within a local transfer, via a remote shell or via a network socket.

- Enable - When checked, proNAS is set as a Rsync server.
- Read only - When checked, all files within this share will be read only to any Rsync client.
- Anonymous - When checked, anonymous connections will be accepted.
- Maximum Connections - This specifies the maximum number of Rsync client that can connect to this share at a certain time.
- Edit accounts - You may edit and existing account, or add/delete a user. These accounts are the accounts that need to be supplied by the Rsync clients when connecting to this server.

Client Mode:

The proNAS system will initiate the synchronization and contact an Rsync server. There are two different ways for Rsync to contact a remote system: using SSH as a remote-shell program as the transport or contacting an Rsync daemon directly via TCP.

- IP Address - This specifies the IP address of the remote Rsync server.
- Remote Path - This specifies the share on the remote Rsync server.
- Account - The valid account name that will be required by the Rsync server for authentication.
- Password - The account's password.
- Mode - Either to download files from the Rsync server or to upload files into the Rsync server.
- SSH - When checked, SSH service will provide the secure tunnel between an Rsync client and an Rsync server.
- Rsync Options - These are the lists of options used during Rsync file transfer



Here is a short summary of the available options. Please refer to the detailed description below for a complete description. Some options only have a long variant.

-r, --recursive	recurse into directories
-v, --verbose	increase verbosity. This option increases the amount of information your are given during the transfer
-l, --links	copy symlinks as symlinks
-p, --perms	preserve permissions. This option causes the receiving Rsync to set the destination permissions to be the same as the source permissions.
-o, --owner	preserve owner (super-user only). This option causes Rsync to set the owner of the destination file to be the same as the source file
-g, --group	preserve group. This option causes Rsync to set the group of the destination file to be the same as the source file.
--ignore-existing	Ignore files that already exist on the receiver. This tells Rsync to skip updating files that already exist on the destination.
-b, --backup	With this option, preexisting destination files are renamed as each file is transferred or deleted. You can control where the backup file goes and what (if any) suffix gets appended using the --backup-dir and --suffix options
--backup-dir=dir	In combination with the --backup option, this tells Rsync to store all backups in the specified directory. This is very useful for incremental backups. You can additionally specify a backup suffix using the --suffix option (otherwise the files backed up in the specified directory will keep their original filenames).
--suffix=SUFFIX	This option allows you to override the default backup suffix used with the --backup (-b) option. The default suffix is a ~ if no --backup-dir is specified, otherwise it is an empty string.
-D, --devices	preserve device files
--specials	preserve special files
-t, --times	preserve times
-S, --sparse	handle sparse files efficiently
-z, --compress	Compresses file data during the transfer. This option is useful in slow links.
-a, --archive	This is equivalent to -rlptgoD. It is a quick way of saying you want recursion and want to preserve almost everything (with -H being a notable omission).
-E, --executability	This option causes Rsync to preserve the executability (or non-executability) of regular files when --perms is not enabled.
-h, --human-readable	Output numbers in a human-readable format.
--stats	Give some file-transfer stats.
--delete	Delete files that don't exist on the sender.
--log-file-format=FORMAT	Output filenames using the specified format.
--log-file=FILE	Output filenames using the specified file.

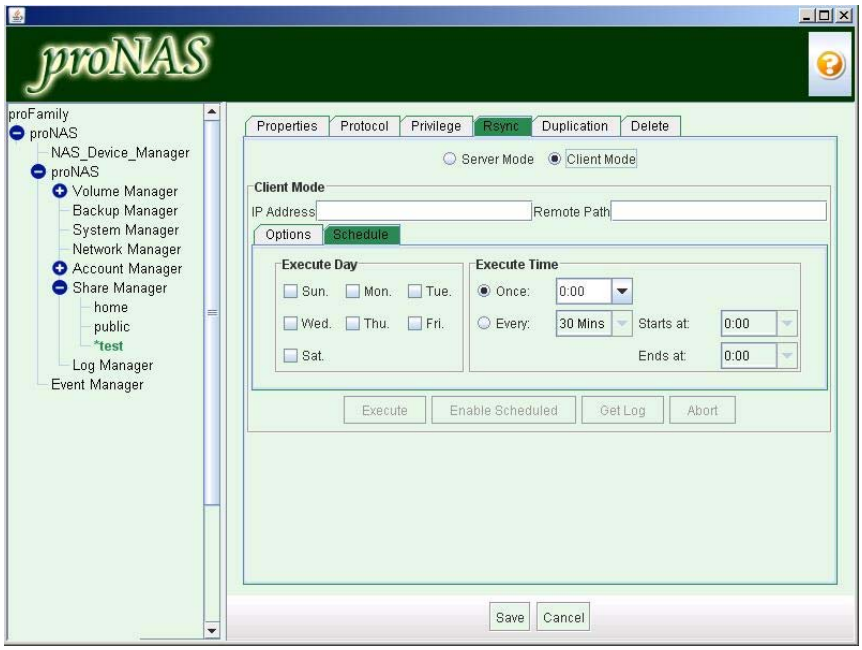
--bwlimit=KB/S	Limit I/O bandwidth; KBytes per second.
-n, --dry-run	This tells Rsync to not do any file transfer; instead it will just report the actions it would have taken.
--timeout=SECS	Sets the maximum I/O timeout in seconds. If no data is transferred for the specified time then Rsync will exit. The default is 0, which means no timeout.

There are lot more useful options that are not included in this list. It may vary depending on your usage, for more information on Rsync, please visit http://samba.org/rsync/.

After completing the above settings, you can run the Rsync client task immediately by clicking the "Execute" button.

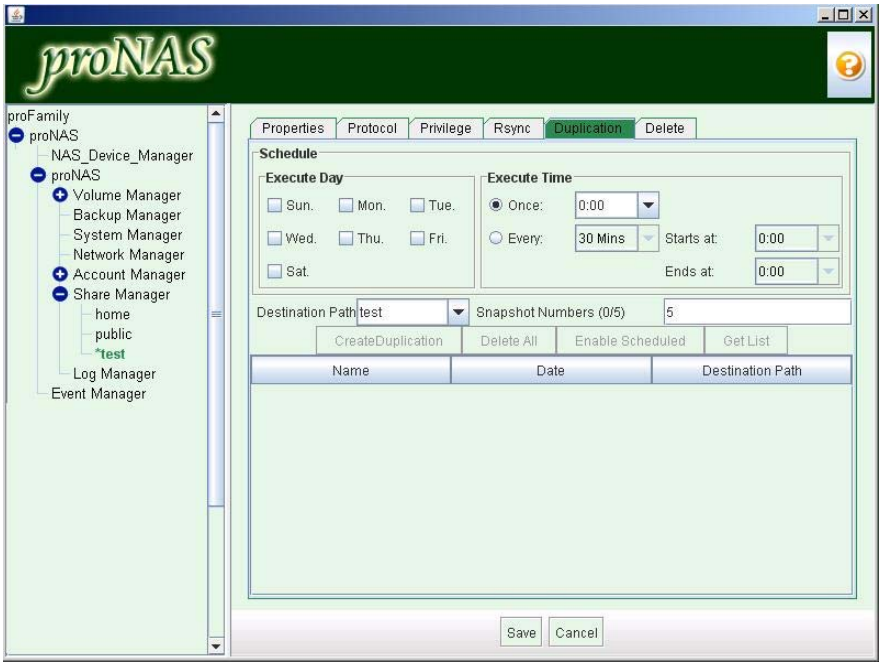
Rsync Schedule

You can automate the Rsync client tasks simply by running it thru schedule. Please select which day(s) to run, the time of the day or if by interval, select a time then set the starting/ending time and then enable the schedule by clicking on the "Enable Scheduled" button.



8.4.6 Duplication

Duplication is a file level snapshot utility for making backups of your local filesystem. Using Duplication, it is possible to take incremental snapshots of your filesystem at different points in time. Duplication creates the illusion of having a multiple full backups by using hard links, while only taking up the space of one full backup plus differences. This saves much more disk space than one might image. The duplication files will be directed to a share which you can access via share protocols or by telnet service. Duplication can be invoked manually or by schedule.
Select the share folder in Share Manager then click “Edit” button.



Creating Duplication by Schedule

To create duplication by schedule, first set the number of total duplication that will be created, specify which day to be run, set the time task whether by interval or once in a specific time of day, set the destination path and then click “Save” button. Enable the schedule by clicking on the "Enable Scheduled" button. To disable the scheduled duplication, just click on the "Disable Scheduled" button.

The Duplication tab information is shown below.

Execute Day:	Specifies whether the scheduled task is to run on this day.
Execute Time:	**Once** - Specifies the time of the day the scheduled task create the snapshot. **Every** - Specifies how often the scheduled task is to be repeated. You can also select the starting time and the ending time.
Destination Path:	This will be the location where your duplication files will be saved. The default path will be the path of the share itself. You can change the path to the other shares except home and public. Duplication will follow the ACL settings of the destination share. If you set the destination of your home duplication to a public share then anybody can access that folders, so please be warned!
Snapshot Numbers:	Specifies the total number of snapshots that can be created. The maximum total number of duplication a share can have is 256.

NOTE: The destination space must be larger than the source. proNAS will check only the destination volume size, not the share usage. Be sure that the available space on the destination is reasonably big enough to accommodate any changes in the source. Home duplication is a special case. If the destination path of the home folder is set to the home itself, its duplication files will only be accessible via NFS or telnet service.

Create Duplication:	This button allows you to create duplication manually.
Delete All:	This button will remove all the duplication files of this share on the current destination path.
Enable / Disable Scheduled:	This button allows you to enable or disable a scheduled task.
Get List:	This button allows you to get the lists of duplications on the current destination path.

Creating Duplication Manually

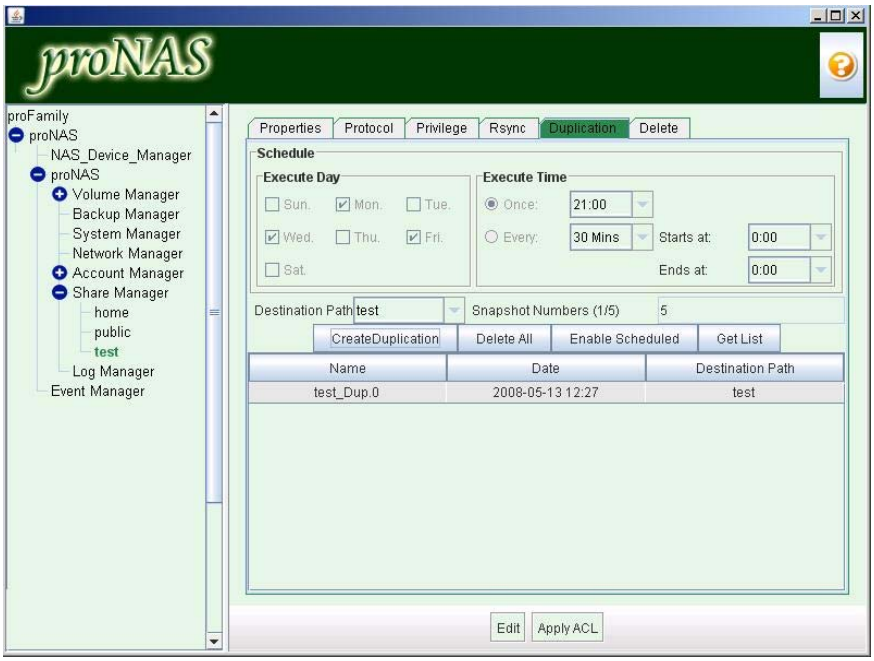
To create duplication manually, first set the number of total duplication that will be created, set the destination path and then click the "CreateDuplication" button. The source share must have at least a single file in order for the duplication to work properly.

Removing or Clearing All Duplication Files

To delete all the duplication files of this share on the current destination path, press the "Delete All" button. Duplication files on the previous destination path will not be removed. Duplication files of other shares on the same destination path will not also be removed.

Getting the Duplication List

To get the lists of all duplication files of this share on the current destination path, please press the "Get List" button. The table will then update the lists of duplication folders. The table includes the date and time it was created and the destination path where it was saved. Duplication files of this share on the previous destination will no longer be included in the list. However proNAS will automatically update the duplication list for you every minute.



How Duplication Works

After you have created Duplication, your destination path will contain a folder "._Duplication". (It is hidden by default, to unhide it, uncheck the "hide duplication" option in the Properties tab of the destination folder). Inside the "._Duplication" folder are the directories that are created for the various intervals that you have defined. It will look something like in the figure below.

Inside each of these folders is the full backup of that point in time of the source share. The format of the duplication folder name will be the share name of the source share appended by an underscore then the character "Dup" followed by the number of the interval. "ShareName_Dup.0" will always contain the most recent snapshot and the duplication with the highest interval number will contain the oldest snapshot. When a new duplication is run, it will rotate all the duplication directories. The files on oldest duplication will not be saved and will be replaced with the content of its succeeding duplication, so please take note of this. The number of duplication will depend on the number of snapshots that you have defined. You need to increase the total number of snapshots if you want to save the backups for a longer time. For example, if you set the snapshot numbers to 60 and you set a schedule to take duplication every day, the very last backup would be around two months old before it will be discharged if a new duplication is made.

NOTE: To view the date modified of duplication folders that corresponds to the date the duplication is taken, use File Manager and view in detailed mode.

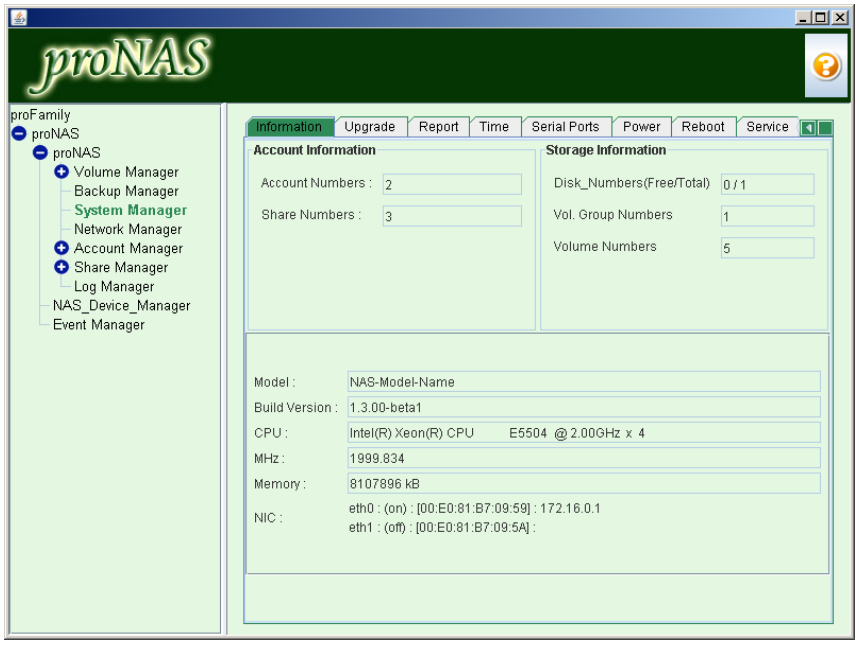
8.4.7 Default Share

Basically, there are there are only two default shares when proNASVG is initially created. If the proBackup Service is started, two other default shares are created. The default shares in proNAS are:

- home - holds the individual shares of all users. It cannot be deleted.
- public - a share intended for all users. Any type of user (including guests or anonymous) can logon to this share and is given read-write permissions.
- proBackupDevice - holds the major backup device for proBackup application. It becomes visible after proBackup service is enabled.
- proBackupExtendedDevice - holds the extended device for other proBackup servers to utilize. It becomes visible after proBackup service is enabled.

8.5 System Manager

System Manager is composed of different tabs which is responsible for the configuration of proNAS system settings and services, such as: Firmware Upgrade, Account and Share reports, Date and Time Zone, Serial Ports and UPS settings, Reboot functions, and Services configurations.



NOTE: Some information shown in the above screenshot may be different from your actual NAS system.

8.5.1 Information tab

The Information tab shows the account, storage and system information.

Account Information

- **Account Numbers** - Indicates the total numbers of all local and external accounts.
- **Share Numbers** - Indicates the total number of all shares.

Storage Information

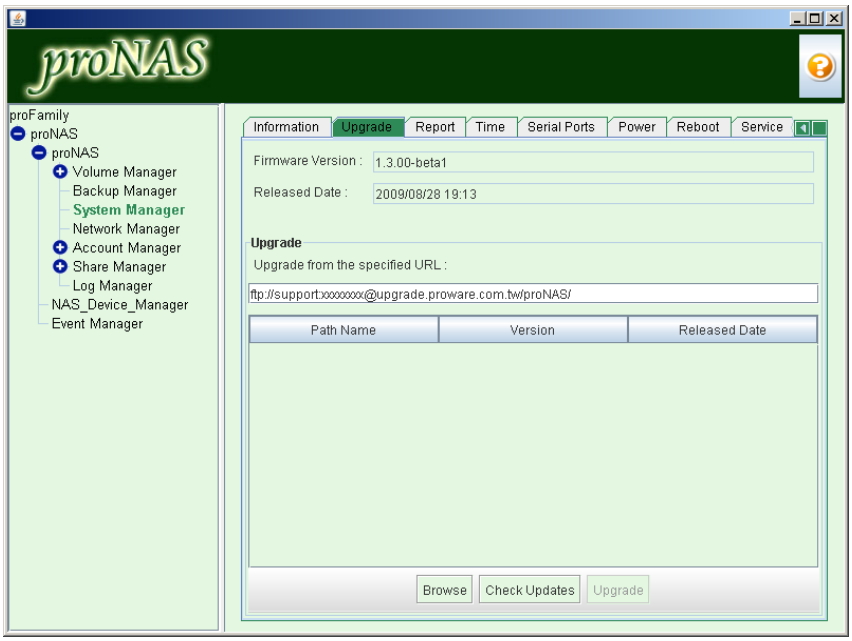
- **Disk Numbers (Free/Total)** - The number of disks in the subsystem, "Free" means the disks those are not joined in volume group.
- **Vol Group Numbers** - The total number of volume groups.
- **Volume Numbers** - The total number of logical volumes. Snapshots will also be counted as volumes.

System Information

- **Model -** Specifies the proNAS system model type.
- **CPU** - Specifies the CPU Type and the number of CPUs.
- **MHz** - Specifies the CPU speed.
- **Memory** - Memory size.
- **NIC** - NIC status, MAC address and IP address.
- **Build Version** - proNAS current firmware version.

8.5.2 Upgrade tab

The Upgrade tab is used to upgrade the proNAS system firmware version.



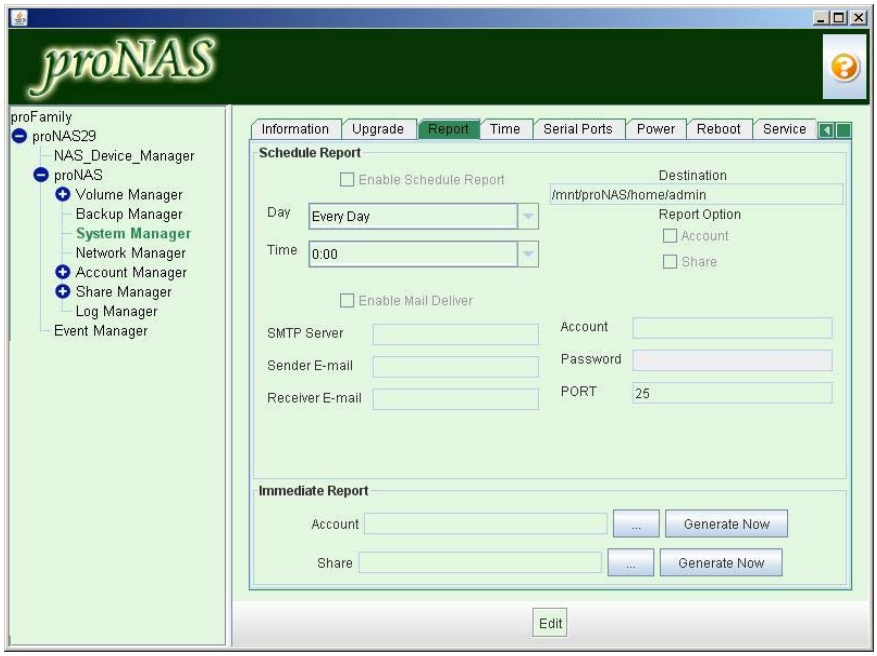
- **Firmware Version** - Displays the current firmware version.
- **Release Date** - The Release Date of this version.
- **Upgrade from the specified URL** - You can download the latest version from URL: ftp://support:xxxxxxxx@upgrade.proware.com.tw/proNAS/

If you would like to see if there is latest version, please press "Check Updates" button. The system will search if there is any latest firmware to update.

Besides firmware update from web-site, you can also do a firmware update from local file system, but you need to download first the firmware patch (Example: proNAS-1.3.00.tar) and save to the local file system. Press the "Browse" button and locate the firmware patch file. Select the patch file when it appears in the list, then click “Upgrade” button.

8.5.3 Report tab

proNAS provides report function which enables you to collect the usage information of all accounts and shares. The output file will be saved in a ".csv" file. Report function can generate report either by schedule or immediately.



Schedule Report

If you would like to enable schedule report, press the "Edit" button, check "Enable Schedule Report", check the report option for "Account" or "Share" or both, and set the Day and Time when to generate the report. The system will generate the report and save in the path /mnt/proNAS/home/admin (The path can be modified).

If you would like to receive the report by e-mail, please check "Enable Mail Deliver" and input the information for SMTP server, sender e-mail and receiver e-mail address. If you prefer to enable email authentication, enter the account and password. You can also change the default port if needed.

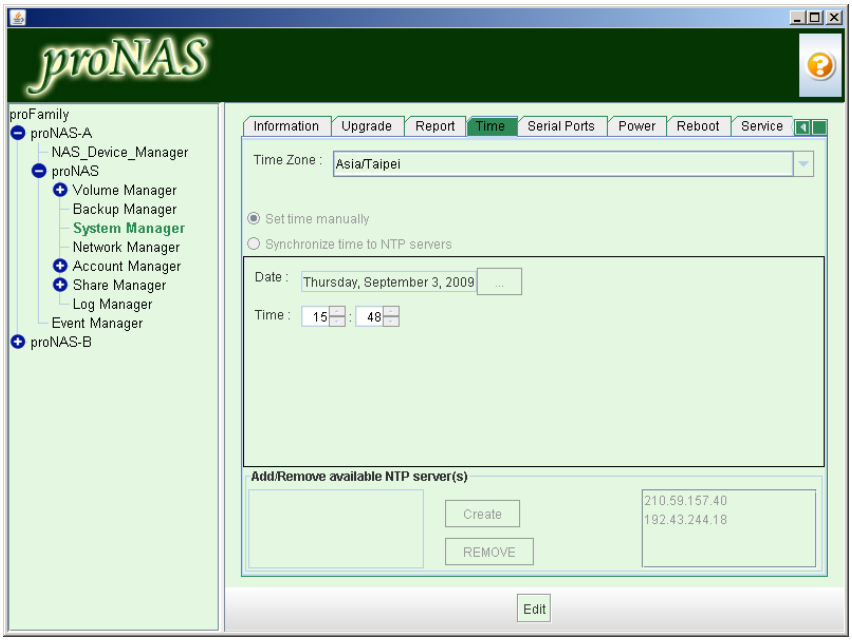
Immediate Report

If you would like to collect the report immediately, press "..." and choose the path for the output file and press "Generate Now" button.

8.5.4 Time tab

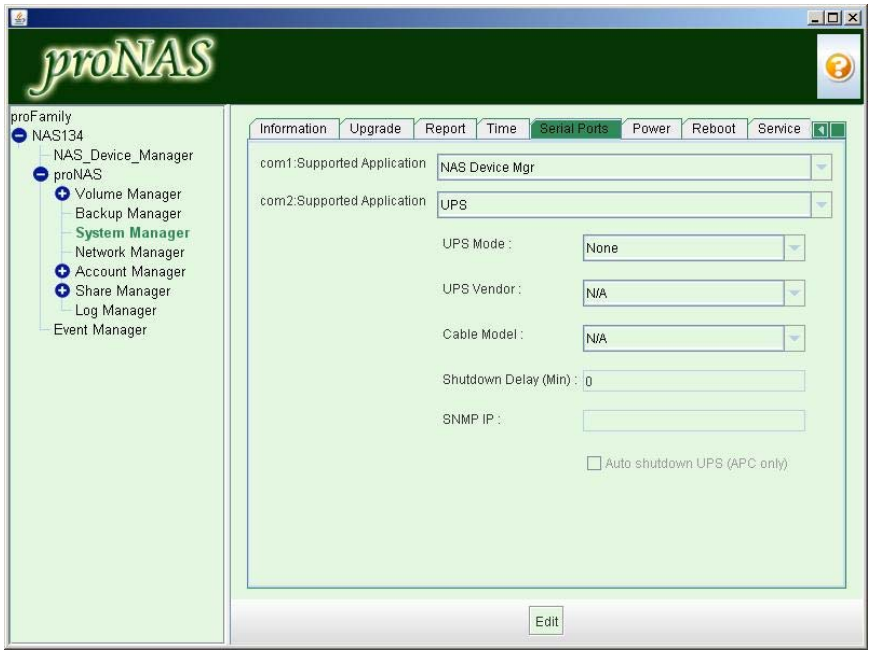
You can configure the system time, date and time zone in this tab. Click the "Edit" button and choose the appropriate time zone. After setting the time zone, select "Set time manually", if not selected, and then set the Date and Time. To set the date, press "...", then the system will display a calendar to choose the date. To set the time, change the hours and minutes.

If you would like to synchronize time with NTP server, select "Synchronize time to NTP servers". The system will display two NTP servers by default. If you would like to add NTP server, enter the NTP server IP address in the “Add/Remove available NTP server(s)” box and press "Create" button. The NTP server will appear in the list of NTP servers on the right column. To remove an NTP server from the list, select the NTP server IP address then press "REMOVE”. When the settings are completed, press "Save" button.



8.5.5 Serial Ports tab

Com1 and Com2 Serial ports can be configured in this tab for specific application. Press "Edit".



Com1

Supported Applications are: NAS Device Mgr or proNAS HA

NOTE: This NAS model does not support NAS Device Manager. You can use COM1 port for proNAS HA (optional) application only.

Com2

Supported Applications are: UPS or proNAS HA

If you set Com2 to UPS, you can select between two supported **UPS Modes:** dumb mode or smart mode.

If you choose dumb mode, you don't have to configure the detail setting about vendor and cable. If you choose smart mode, proNAS supports three **UPS Vendor:** (a) APC, (b) BeamTech, and (c) HyperPro. Select the UPS vendor then set the **UPS Model** and **Cable Model**. The only Beamtech UPS model supported is SSpro 650. The only HyperPro UPS model supported is 1410HP. APC has many models supported. APC cable models are: simple, smart, ether, usb, and snmp

Shut Down delay (Min): the time to shutdown system after power fail

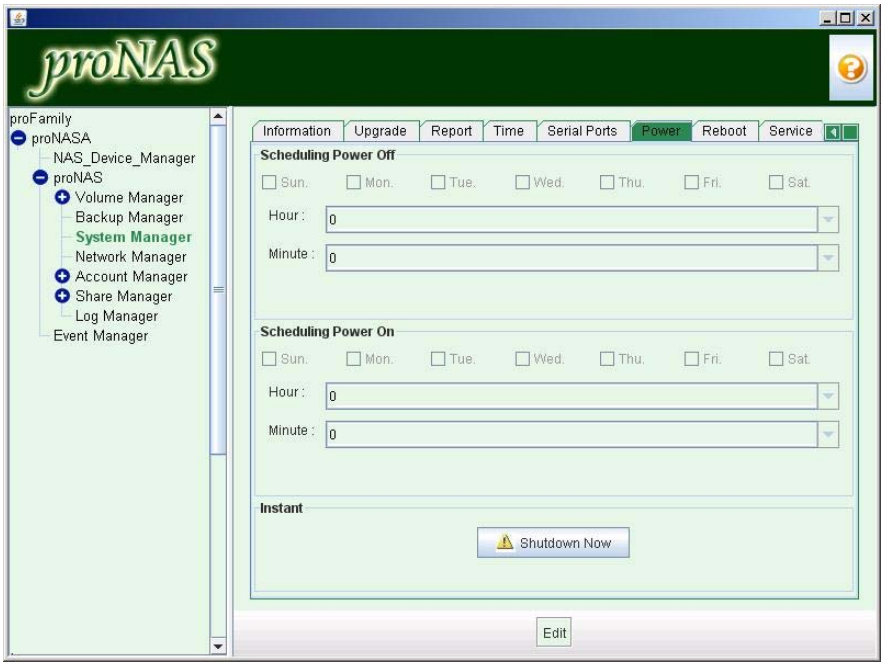
SNMP IP: the IP address of APC UPS. This is enabled when cable model is set to snmp.

Auto Shutdown UPS (APC only): automatically shutdown system after power fail; APC UPS only

After completing the settings, press "Save" button.

8.5.6 Power tab

The Power tab is used to configure schedule system power off and power on. You can also shutdown the system immediately using “Shutdown Now” button.



Scheduling Power Off

Select the day or days, and set the Hour and Minute when the system will shutdown.

Scheduling Power On

Select the day or days, and set the Hour and Minute when the system will power on.

Instant

To shutdown the NAS immediately, click “Shutdown Now” button.

8.5.7 Reboot tab

The administrator can reboot proNAS by schedule or immediately.

If you would like to reboot by schedule, press "**Edit**" button, and check "**Enable schedule reboot**". Choose the date and time when to reboot. This function can help to clean the unnecessary system process or connection periodically.

If you would like to shut down or reboot immediately, press "**Shutdown Now**" or "**Reboot Now**":

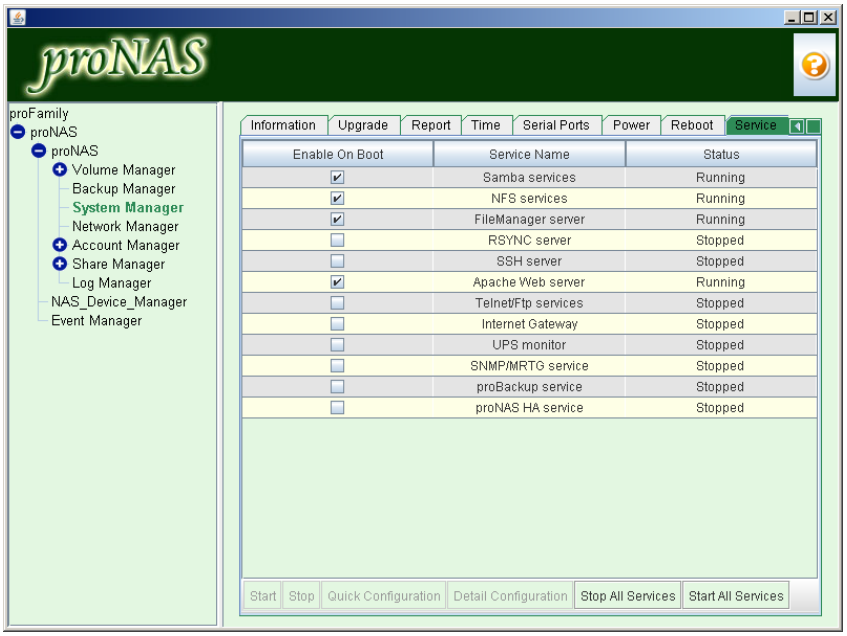
If you check there is file error or I/O error from system log, or VG cannot mount, or system shutdown abnormally, it is recommended to use the function "**Reboot & File System Check**".

If you would like to erase existing storage and proNAS configuration and reset to factory default, you can use the "**Erase Storage & Configuration**" button.

WARNING! All data and configuration will be deleted if you use this function. Please make sure you already have a backup of your data and configuration, or that you do not need the current data and configuration.

8.5.8 Service tab

The various proNAS services can be set in this tab.



If you would like to enable service while booting, please check "Enable on Boot" option. You can also press "Start All Services" button to run all services, or press "Stop All Services" button to stop all services. If you would like to enable or disable certain service, please select the service item and press "Start" button or "Stop" button.

proNAS system services are as follows:

Samba services:	Provides CIFS file sharing, MS Windows users need this to access proNAS.
NFS service:	Provides NFS file sharing, UNIX users need this to access proNAS.
File Manager server:	Enables to stop and start the File Manager web page service.
RSYNC server:	Provides Rsync process or system to which the Rsync client connects. **NOTE: By default, charset is set to UTF8 in Rsync configuration.**
SSH server:	Provides remote management with more secure level.
Apache Web server:	This provides web service for proNAS use. You need to enable this service always. The default port number used is 80.

Telnet/Ftp service:	Provides users access proNAS with telnet or ftp **NOTE: By default, maximum number of Telnet and FTP connections is set to unlimited.**
Internet Gateway:	Provides Internet access.
UPS monitor:	If you would like to connect UPS, you have to enable this service.
SNMP/MRTG service:	Provides SNMP/MRTG service to view system information. proNAS can send trap messages if: - A logical volumes becomes almost full (ID 128) - A snapshot volume becomes almost full (ID 129) - A replication is disconnected (ID 130)
proBackup service:	Provides service for NAS users to backup their files to NAS. Refer to Chapter 11 for fore information.
proNAS HA service:	Provides NAS HA solution.

proNAS provides "Quick Configuration" for administrator to configure service parameters. Experienced administrator can also configure the advance settings in "Detail Configuration".

proNAS Quick Configuration options are as follows:

Samba Service

- Strict allocate setting – This option controls the handling of disk space allocation in the proNAS server. When strict allocate is set to “no” (default setting) the server does sparse disk block allocation when a file is extended.

File Manager Server

- Languages – This option allows selecting the language to be used by File Manager. Options are: English and Traditional Chinese.

SSH Service

- Allows root login via SSH service
- Enable SFTP

The default settings of 2 options are set to “no”. If necessary, change the setting from “no” to “yes” then Save.

Apache Web Service

- IP Port – The port number used by apache web server. Default port number is 80.

Telnet / FTP services

- Allows root login via FTP
- Allows root login via Telnet

The default settings of 2 options are set to “no”. If necessary, change the setting from “no” to “yes” then Save.

SNMP / MRTG Service

- Trap Receiver IP: Enter the IP address of the SNMP trap receiver.

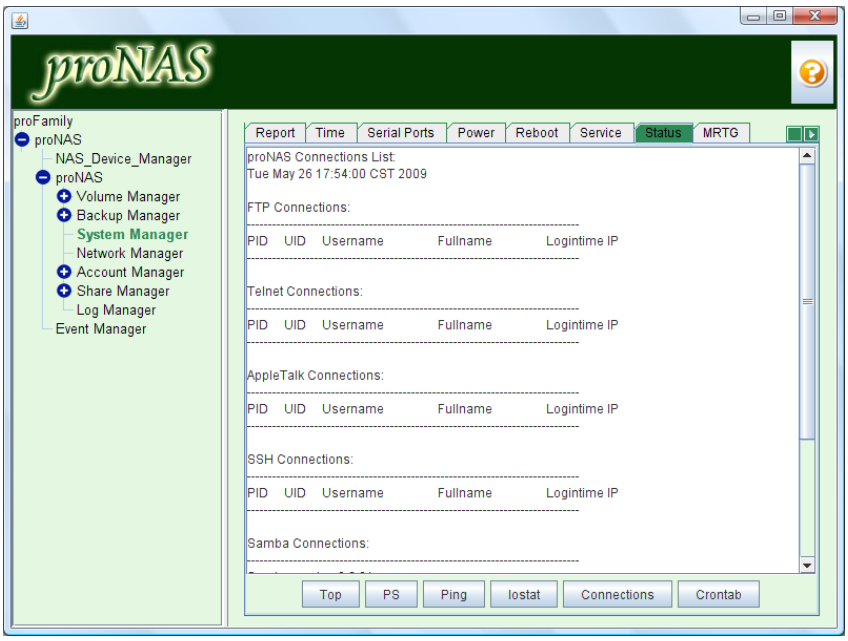
proBackup Service

- IP of Rx/Tx backup streams: Enter the proNAS network interface IP address for proBackup service stream
- Port of Rx/Tx backup streams: Enter the Port number for proBackup stream, default is 1089.

8.5.9 Status tab

You can use this tab to view system status, such as various Service Connections, Top, PS, and Iostat, to perform network test (Ping), or to view Crontab schedule.

By default, a summary of connections and resources used for local and remote computers is listed. The information includes the PID, User, User full name or comment, login time, and the IP address of the connected computer. You can click the "Connections" button to display current connection list.



Click the "**Top**" button to display system summary information and tasks list.

Click the "**PS**" button to display information about active processes.

Click the "**Ping**" button to perform network test. A dialog box will be displayed. Enter the IP address then click "Start". The ping result will be shown in the Status area.

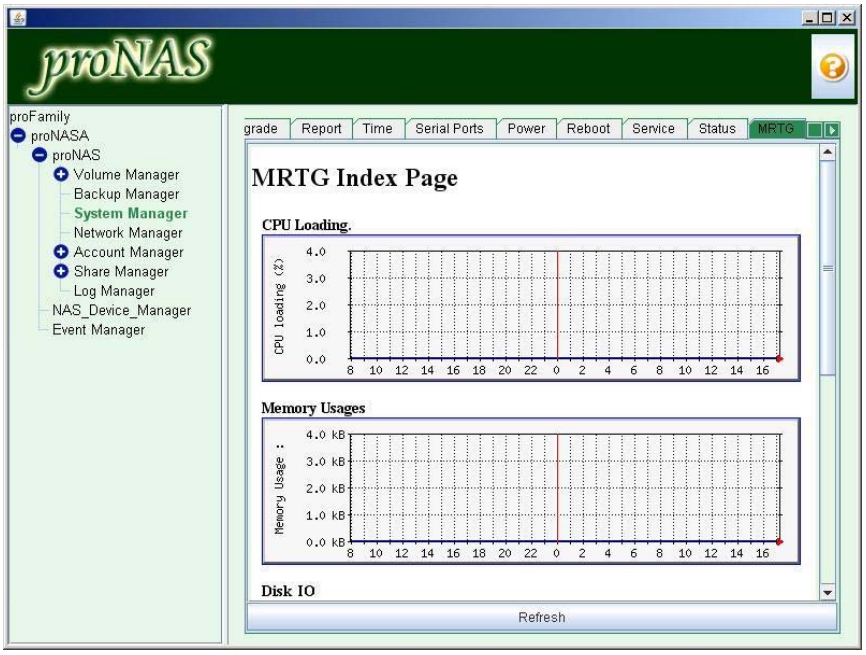
Click the "**Iostat**" button to display system input/output device loading, specifically storage and disk device statistics.

Click the "**Connections**" button to display current connection list.

Click the "**Crontab**" button to display a list of Crontab schedule.

8.5.10 MRTG tab

This tab shows information about MRTG graphs and includes CPU Loading, Memory Usage, Disk IO, and Network Traffic.

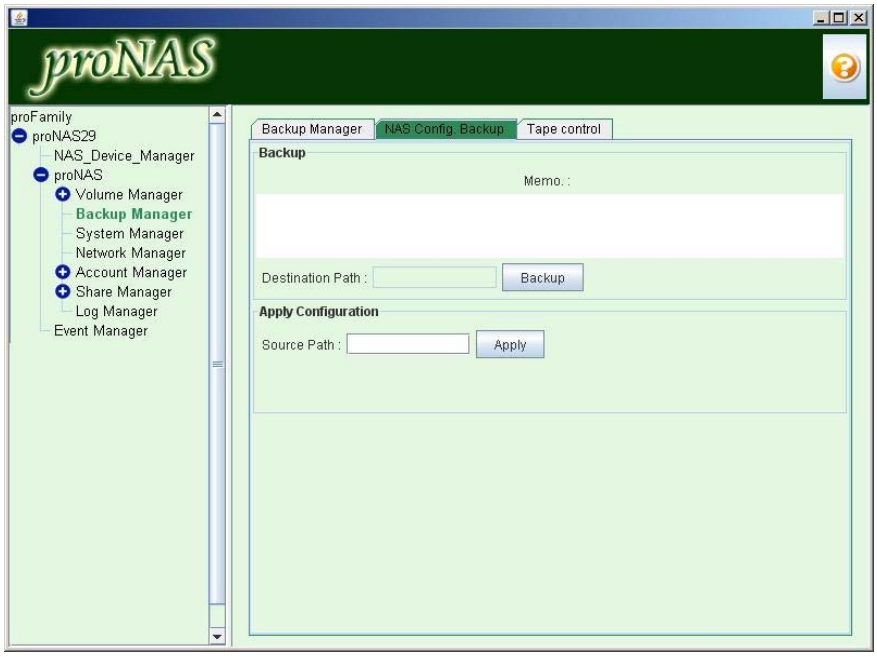


8.6 Backup Manager

You can backup proNAS data and system configuration via Backup Manager.
In "Backup Manager" tab, you can check the existing backup plans in the "Backup Plan List" which includes backup plan name, next backup time and if the backup plan schedule is enabled. If you would like to create new backup plan, please press "Add Backup Plan" button.

8.6.1 proNAS Configuration Backup

proNAS provides System Configuration Backup which means administrator can backup system configuration information. Select "NAS Config Backup" tab.



Press "Backup" button. Choose the path you would like to save the file and enter the file name. System will backup the configuration information as an .xml file. If you would like to restore the configuration later, press "Apply" button.

NOTE: Not all proNAS configuration will be included in NAS Config backup. These includes Replication, Snapshot, Event Manager setting and HA configurations.

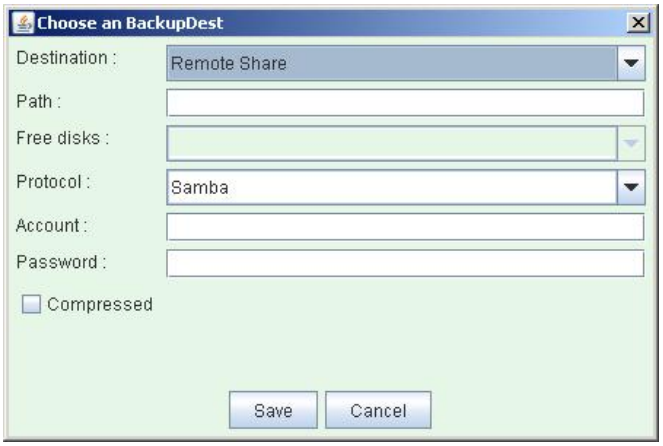
NOTE: Before you can restore a NAS backup configuration, you need first to reset the NAS to factory default settings. And make sure you have made a backup of all needed data.

8.6.2 Configure Backup Plan

Backup Plan Setting

In the "Backup Plan Setting" tab, you can create new a backup plan. Enter the "Backup Plan Name", and then press "..." to choose the backup destination, your destination could be remote share, tape or local device.

NOTE: If a disk is already selected as Local Device backup destination, the disk status in Volume Manager will change to "BACKUP". This disk will not be available in the Free Disks list at Destination option.



Use the following guidelines to ensure that you are using a valid backup plan name:

- Names cannot be longer than 256 characters.
- Names should be unique. It cannot be a duplicate with other Backup plan names.
- Names cannot contain blank spaces.
- Names cannot begin with a dash (-) and cannot consist of only a single dash.
- Names cannot contain the following characters: /\[]";:|<>+=,?*

If you choose remote share, please input the IP address in the "path" field. Choose Samba or NFS of the protocol and enter account and password.

Example:

For Samba:

Path = //192.168.100.164/Share	You cannot use the directory under the share. Example: //192.168.100.164/Share/dir1 <==Incorrect //192.168.100.164/Share <==Correct If you are not sure of the share name on the remote machine, you may query it by using the command "smbclient". -bash-3.00# smbclient -L 192.168.100.164
Login = account	Account that has full access permission on the remote share.

For NFS:

Path = 192.168.100.164:/PathToShareName	Example: 192.168.100.164:/mnt/proNAS/vol1/share1 If you are not sure of the correct path of the remote NFS server, you may use the command "showmount". -bash-3.00# showmount -e 192.168.100.164
Login	For NFS, it will assume the root account to be used. Please verify that root account can access the remote NFS share.

If Backup Manager fails to mount the remote share, you may need to verify it manually via console. That is to connect to the remote machine and mount the remote share. First we need to create a directory as our mount point.

```
-bash-3.00# mkdir /mnt/temp/
```

For Samba:

```
-bash-3.00# mount //ServerIP/ShareName /mnt/temp -o lfs,
                                    username=account,password=password
```

For NFS:

```
-bash-3.00# mount ServerIP:/PathToShareName /mnt/temp
```

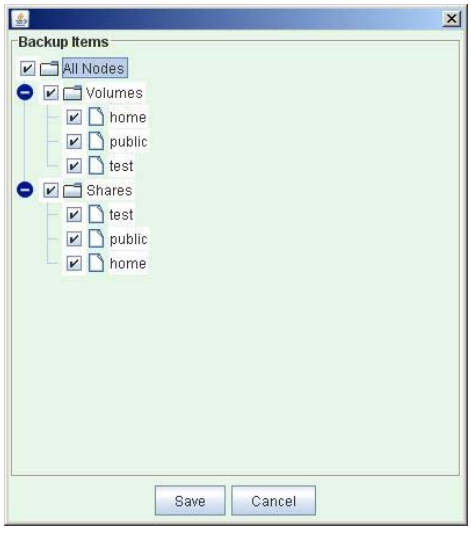
If you choose tape, you don't need additional setting.

If you choose local device, the system will display the available disks in the "Free Disk" field. When this backup configuration is saved, a “format local disk” confirmation window will be displayed.

If you choose the option "compressed", the data will be compressed to * .gz file.

Press "Save” button complete the setting and go back to "Backup Plan Setting" tab. In the field of "Description", system will display your backup destination (remote share / tape / local disk) in Type area.

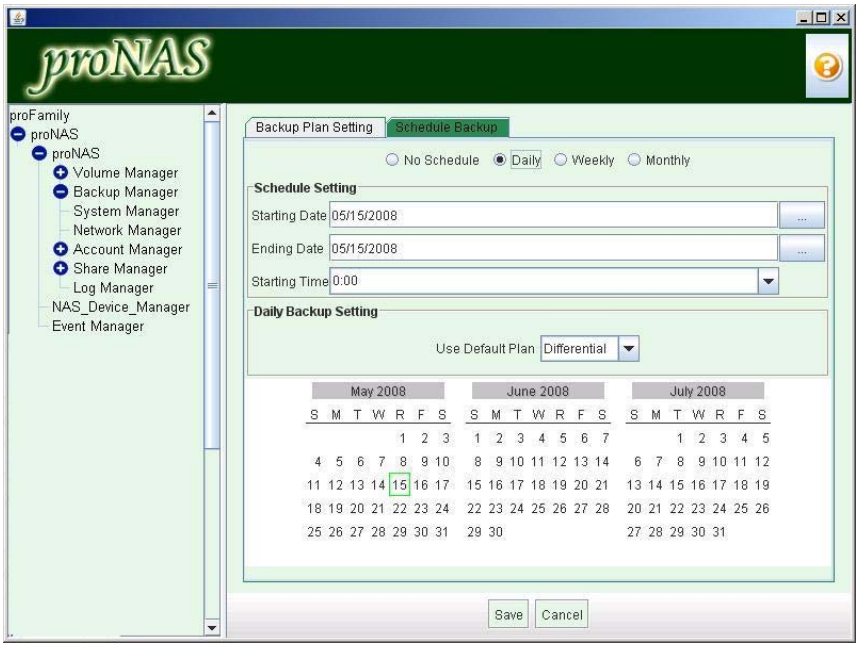
Please press "Edit Backup Item List" button. System will display the window for you to choose the backup items ("Volumes" or "Share"). Choose your backup items and press "Save" button to go back to "Backup Plan Seting" tab. You can check the backup items in the "Backup Item(s)" list, if you would like to remove some items. Please check in the "Remove" filed and press "Remove Backup Item(s)".



Schedule Backup tab

After you complete the above setting, you can setup the schedule in the "Schedule Backup" tab, if the tab, you will see the option of "No Schedule", "Daily", "Weekly", and "Monthly".

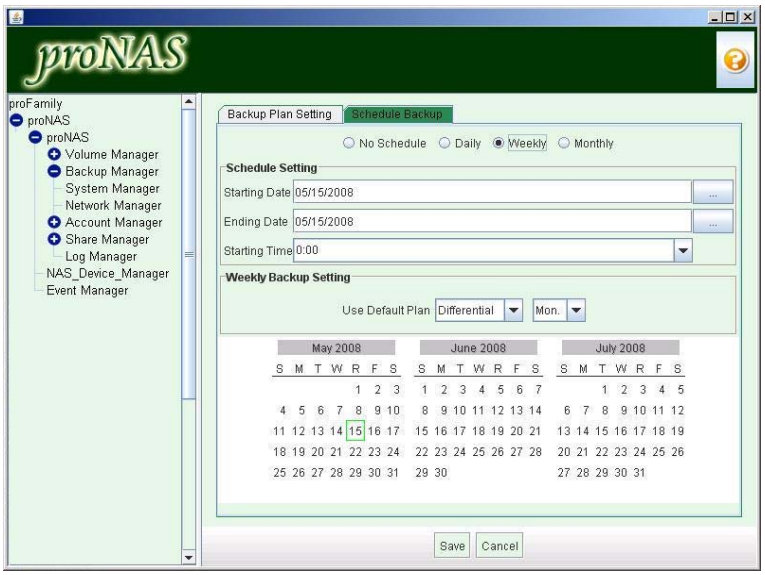
- **Daily**: If you would like to do the backup every day, please check "Daily". Please press"...", system will display the calendar. You can choose "Start Date" and "Ending Date" and the "Starting time".



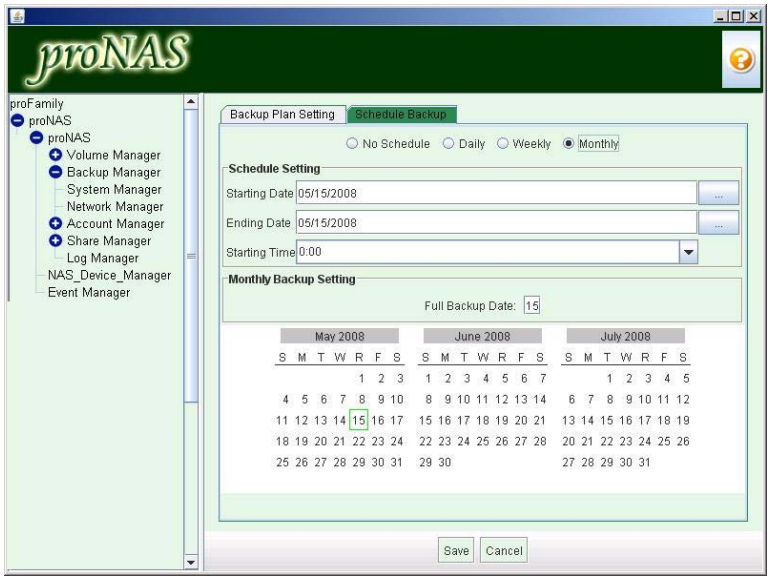
proNAS provides 3 kinds of backup methods:

- Incremental: An incremental backup stores all files that have changed since the last backup. The advantage of an incremental backup is that it takes the least time to complete. However, during a restore operation, each incremental backup is processed, which could result in a lengthy restore job.
- Differential: A differential backup contains all files that have changed since the last FULL backup. The advantage of a differential backup is that it shortens restore time compared to a full backup or an incremental backup. However, if you perform the differential backup too many times, the size of the differential backup might grow to be larger than the baseline full backup.
- Full: Full backup

- **Weekly**: If you would like to backup weekly, please check this option. Please press "...", system will displays the calendar. You can choose "Start Date" and "Ending Date" and the "Starting time".



- **Monthly**: Full backup is the starting point for all data backup. Choose this option to do full backup monthly.



Press "Save" after you completed the settings. Go back to "Backup Plan Setting" tab. You will see the backup plan in the "backup plan list".
If you would like to modify the backup plan, please choose the backup plan in the left tree-node, and press "Edit". If you would like to backup immediately, please press "Backup Now"; or press "Enable schedule backup". System will display schedule enable or disable in "Backup Status" field.
If you would like to restore data from the backup plan, please choose the backup plan in the left tree-node, and go to "Restore" tab, press "Restore" button.

8.6.3 Tape Control

The Tape Control tab allows you to control the tape function when attached to the NAS.

Options:

rewind tape to the begin. – This enables the tape to be rewound to the beginning of the tape.

forward tape to the end of data – This enables the tape to be forwarded to the end of data.

erase all data in tape – This enables the data on the tape to be erased.

eject tape – This enables the tape to be ejected from tape drive.

Status – This shows some information about current status of tape, such as tape is online.

When using the rewind/forward/erase/eject option, a confirmation message will be displayed. You can select “Yes” to continue, or “No” to cancel.

NOTE: Backup to tape has the following features:

1. **Backup across 2 tapes**

   When doing backup of large data and the first tape cartridge becomes full, the backup can continue by inserting another tape cartridge.

2. **Multiple backup**

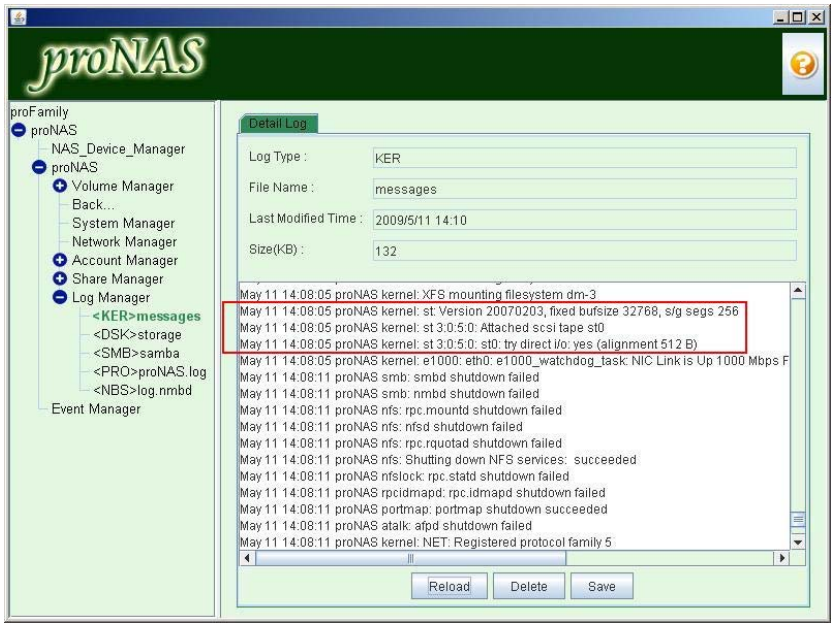
   When doing backups, it can be done many times. That is, a backup plan can be executed many times and the backup data will be saved one after the other in the tape cartridge.

8.6.3.1 Backup and Restore Using Tape

Here are sample procedures how to create backup to tape drive, or restore backup.

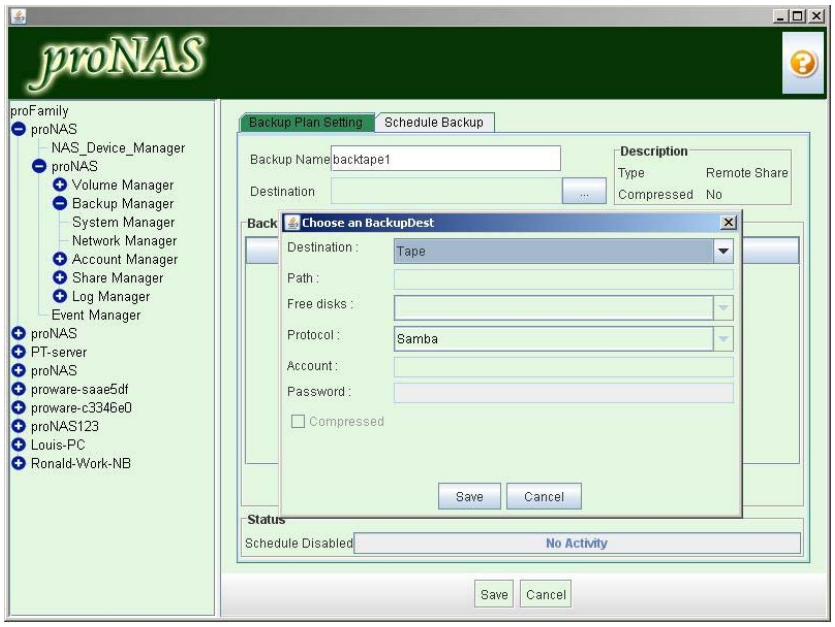
A. Preparing the NAS and Creating Backup Plan

1. Connect the Tape Backup device to the available Tape (SCSI) port on the NAS. Note that you need to shutdown the NAS before connecting the Tape Backup device.
2. After boot-up of NAS, check in the Log Manager (<KER>messages) if the tape device has been detected.


proNAS
proFamily
proNAS
NAS_Device_Manager
proNAS
Volume Manager
Back...
System Manager
Network Manager
Account Manager
Share Manager
Log Manager
<KER>messages
<DSK>storage
<SMB>samba
<PRO>proNAS.log
<NBS>log.nmbd
Event Manager
Detail Log
Log Type : KER
File Name : messages
Last Modified Time : 2009/5/11 14:10
Size(KB) : 132
May 11 14:08:05 proNAS kernel: XFS mounting filesystem dm-3
May 11 14:08:05 proNAS kernel: st: Version 20070203, fixed bufsize 32768, s/g segs 256
May 11 14:08:05 proNAS kernel: st 3:0:5:0: Attached scsi tape st0
May 11 14:08:05 proNAS kernel: st 3:0:5:0: st0: try direct i/o: yes (alignment 512 B)
May 11 14:08:05 proNAS kernel: e1000: eth0: e1000_watchdog_task: NIC Link is Up 1000 Mbps F
May 11 14:08:11 proNAS smb: smbd shutdown failed
May 11 14:08:11 proNAS smb: nmbd shutdown failed
May 11 14:08:11 proNAS nfs: rpc.mountd shutdown failed
May 11 14:08:11 proNAS nfs: nfsd shutdown failed
May 11 14:08:11 proNAS nfs: rpc.rquotad shutdown failed
May 11 14:08:11 proNAS nfs: Shutting down NFS services: succeeded
May 11 14:08:11 proNAS nfslock: rpc.statd shutdown failed
May 11 14:08:11 proNAS rpcidmapd: rpc.idmapd shutdown failed
May 11 14:08:11 proNAS portmap: portmap shutdown succeeded
May 11 14:08:11 proNAS atalk: afpd shutdown failed
May 11 14:08:11 proNAS kernel: NET: Registered protocol family 5
Reload
Delete
Save

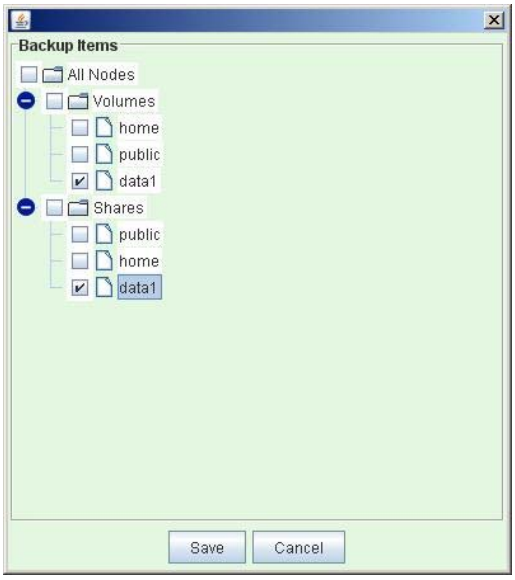
3. Select Backup Manager. Click “Add Backup Plan”.

4. Enter a Backup Name. In Destination, click "..." button. In the dialog box that appears, select "Tape" as backup destination. Click "Save".

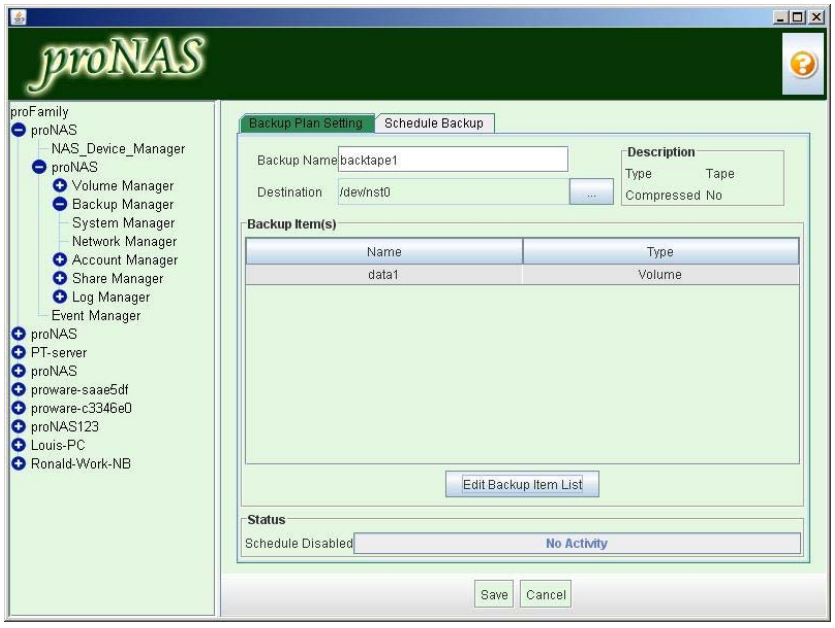


5. The destination (tape device) is set. Click "Edit Backup Item List".

6. Select the data (Volume/Share) to be backed up. Click “Save”.



7. Click “Save” again.



8. In the Confirm Dialog Box, click “Yes”.

9. Insert the tape cartridge into the tape drive.

Take note of the following proNAS tape control functions as follows:

rewind tape to the begin. – This enables the tape to be rewound to the beginning of the tape.

forward tape to the end of data – This enables the tape to be forwarded to the end of data.

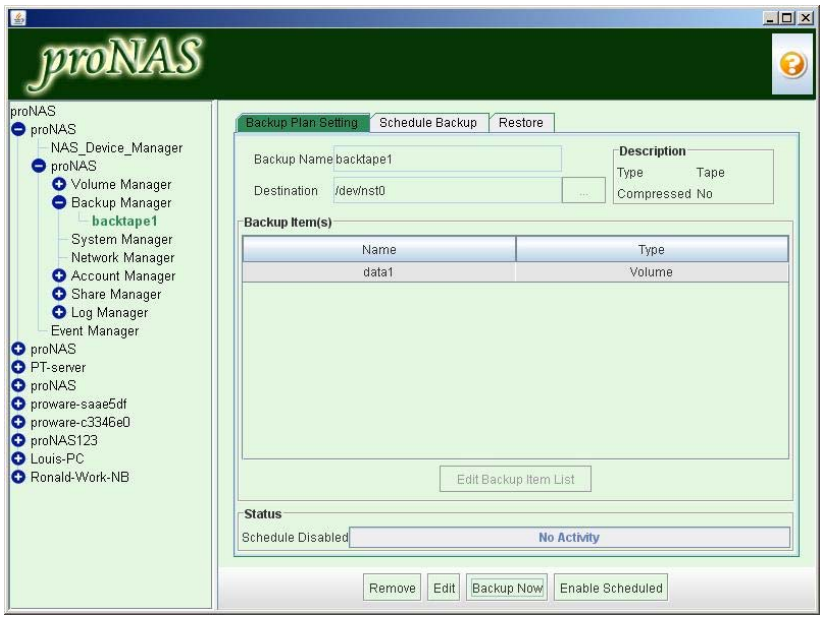
erase all data in tape – This enables the data on the tape to be erased.

eject tape – This enables the tape to be ejected from tape drive.

Status – This shows some information about current status of tape, such as tape is online.

B. Manual Backup and Restore

1. Select the backup plan under Backup Manager.



2. Click “Backup Now”. In the dialog box, click “Yes” to confirm.

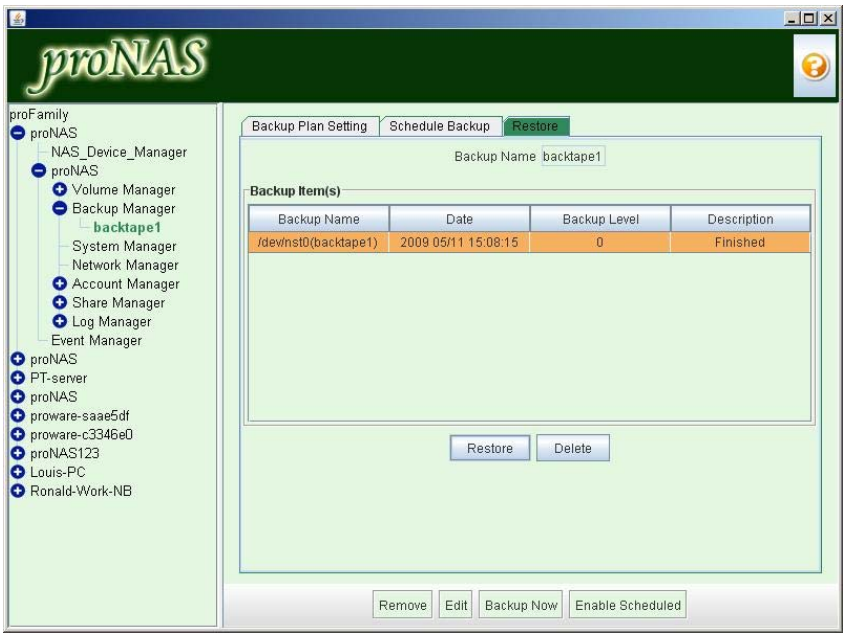
3. The backup process will be started.

4. When backup is completed, a message will be displayed. Click “OK”.

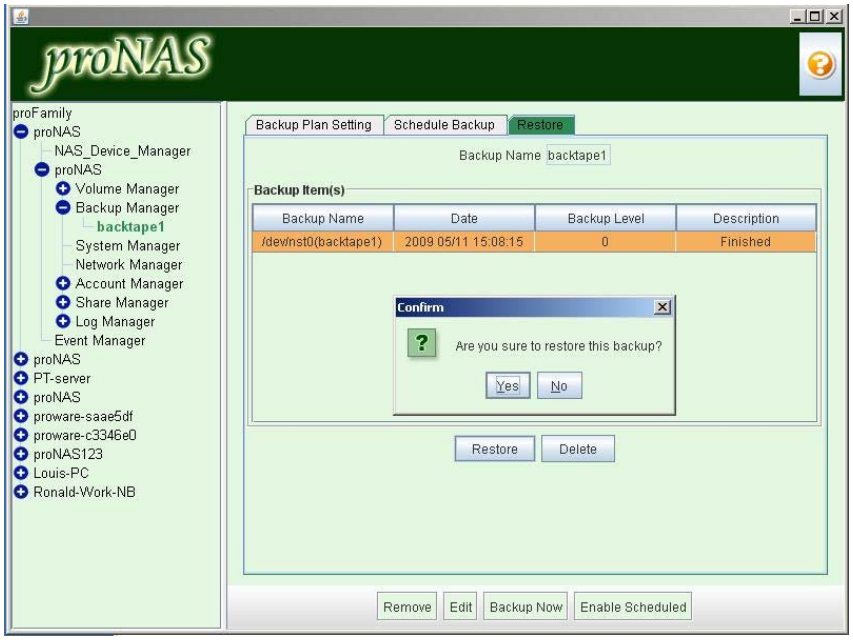
5. To check the backup made, while in the backup plan name, select Restore tab.

6. To restore data, try to delete old data from the share folder.

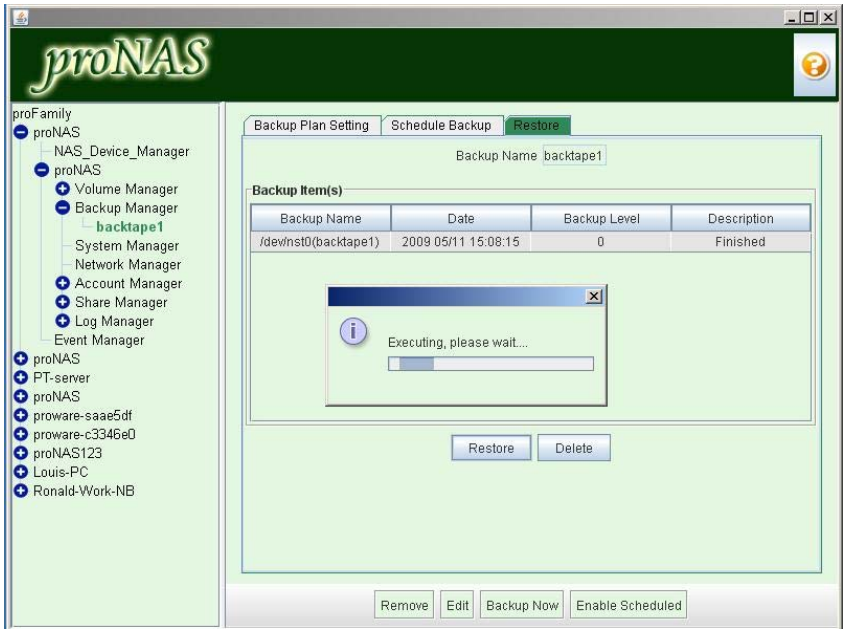
7. To restore data from tape backup, in Restore tab, select the backup name from backup Item(s) then click “Restore”.



8. In the dialog box, click “Yes” to confirm.

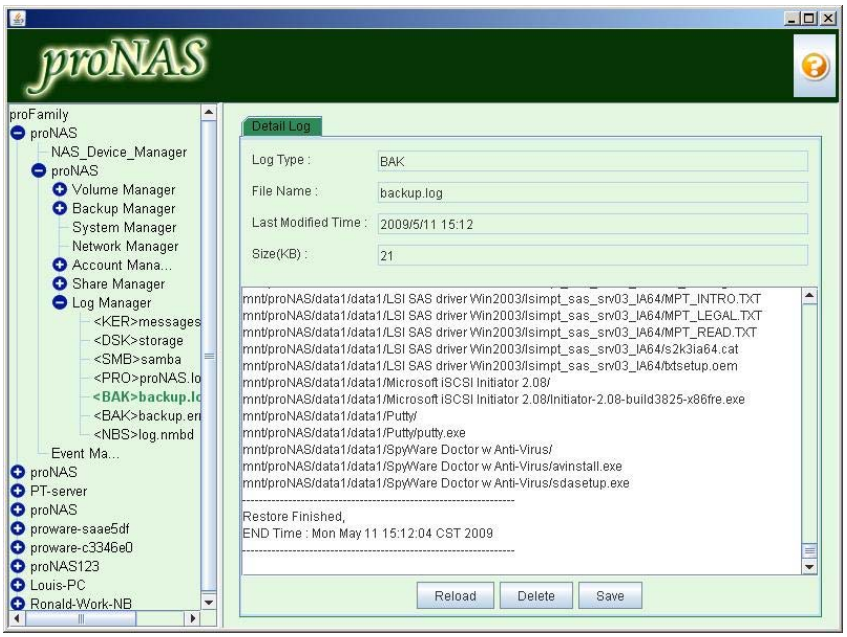


9. The process of restoring data will be started.



10. When restore is completed, a message will be displayed.

11. To verify restore process from log, select Log Manager then “<BAK>backup.log”.



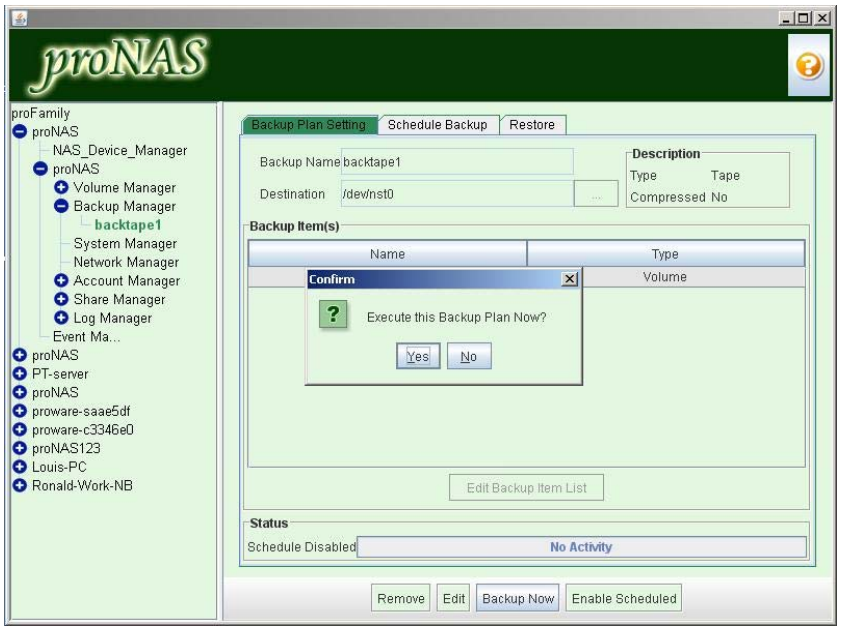
12. Check the share folder if it contains the old data.

C. Creating Multiple Manual Backups

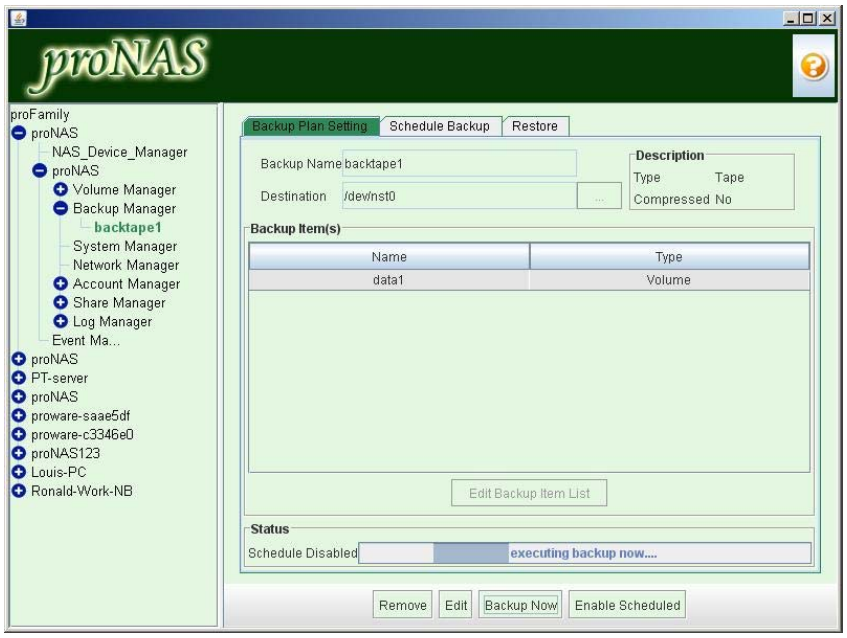
NOTE: Manual backups are always Full backup, which means their Backup Level is always 0 (zero).

1. Update (copy and/or delete) some data to the share folder.

2. Select the backup plan then click “Backup Now”. Select “Yes” to confirm.



3. The backup will be executed.



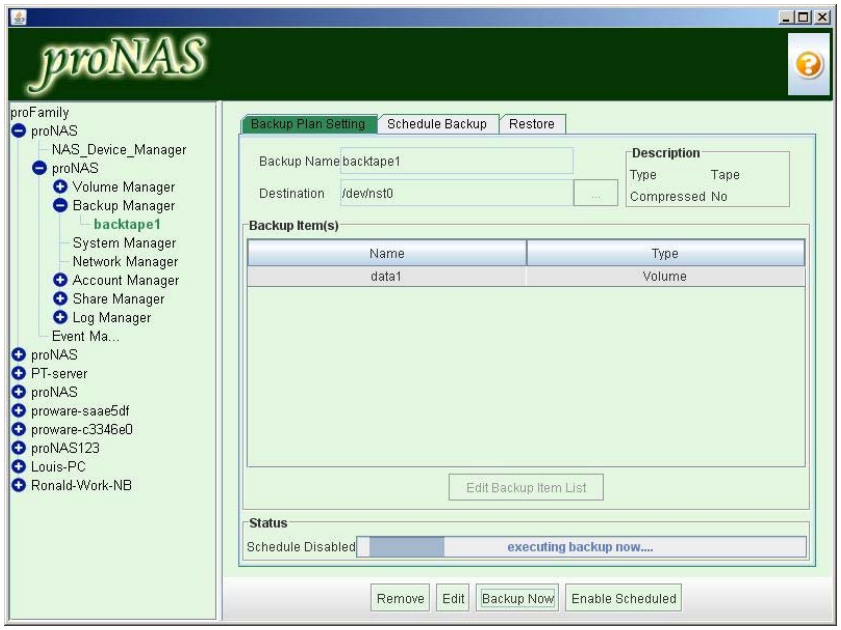
4. A message will be displayed after backup is completed.

5. A second backup is created.

6. Update (copy and/or delete) some data to the share folder.

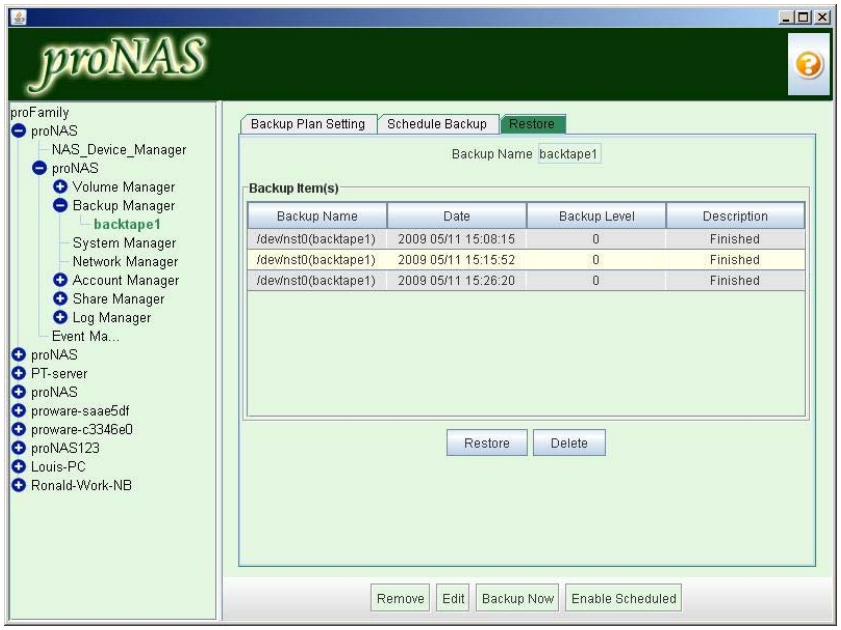
7. Click “Backup Now”. Select “Yes” to confirm.

8. The backup process will start.



9. When completed, a message will be displayed.

10. In Restore tab, check the backup items. Note that the Backup Levels are 0.

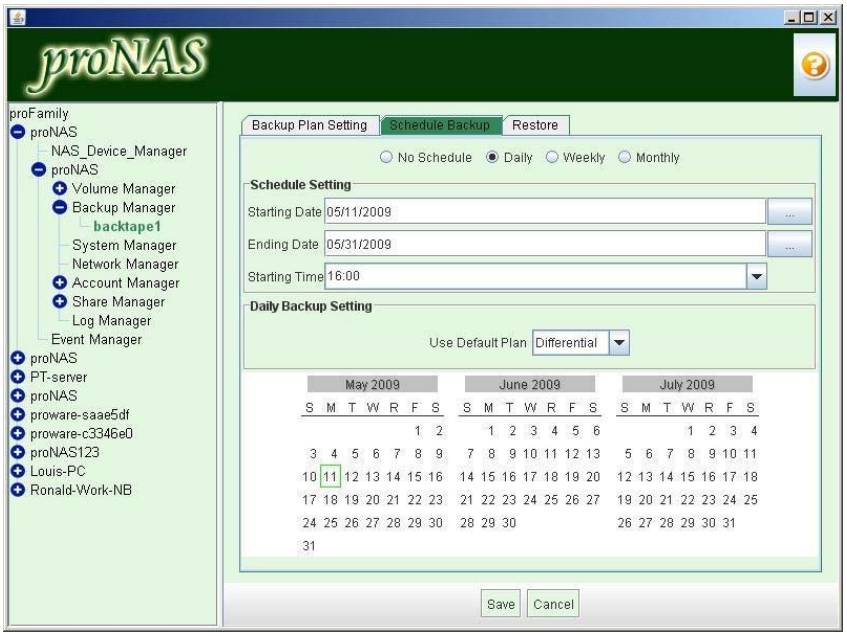


11. The backup items can be restored or deleted.

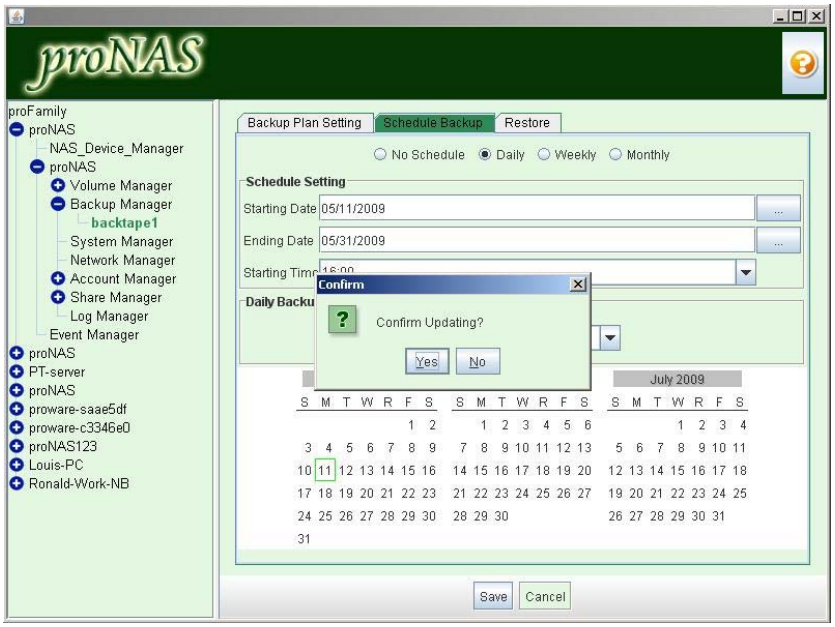
D. Backup by Schedule

1. Create a backup-to-tape backup plan (set destination to tape, and select backup items). Then click “Edit”.

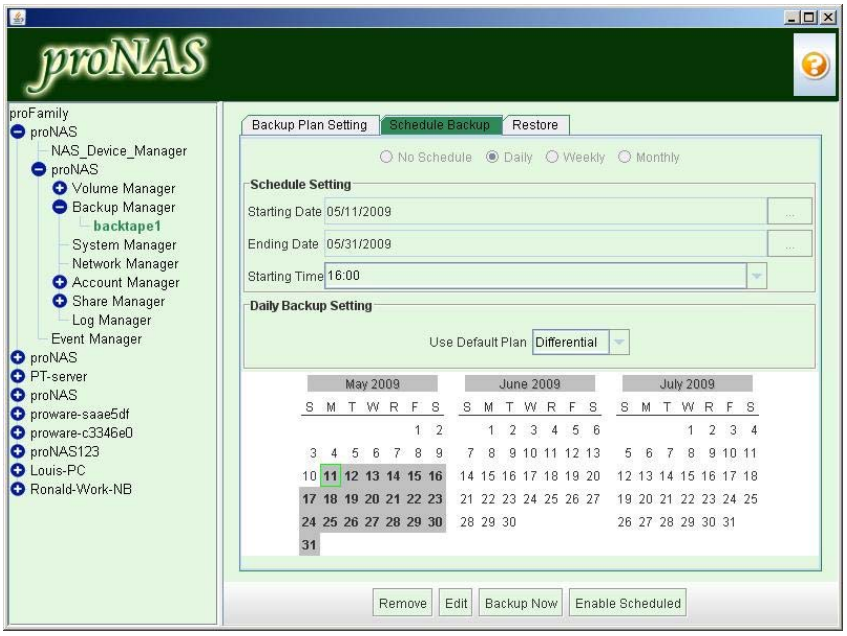
2. Select “Schedule Backup” tab. Select the backup frequency (Daily, Weekly, or Monthly). Set the starting date, ending date, and starting time. Specify the backup type in Use Default Plan option. For example, in Daily backup, you can select Differential, Incremental, or Full.



3. Click “Save” when done. Select “Yes” to confirm.

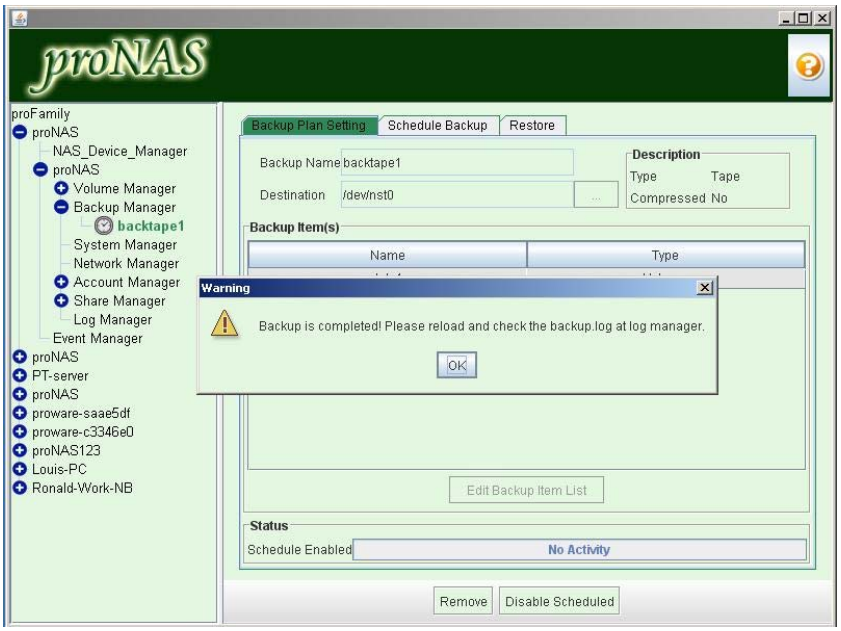


4. Scheduled backup has been configured.



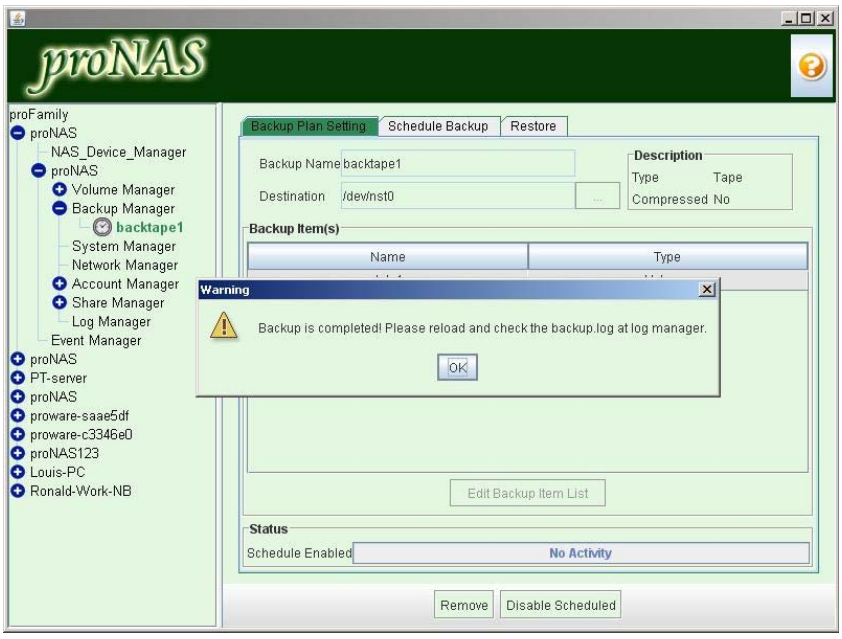
5. To enable the scheduled backup, click “Enable Scheduled”. A clock icon will appear beside the name of backup plan.

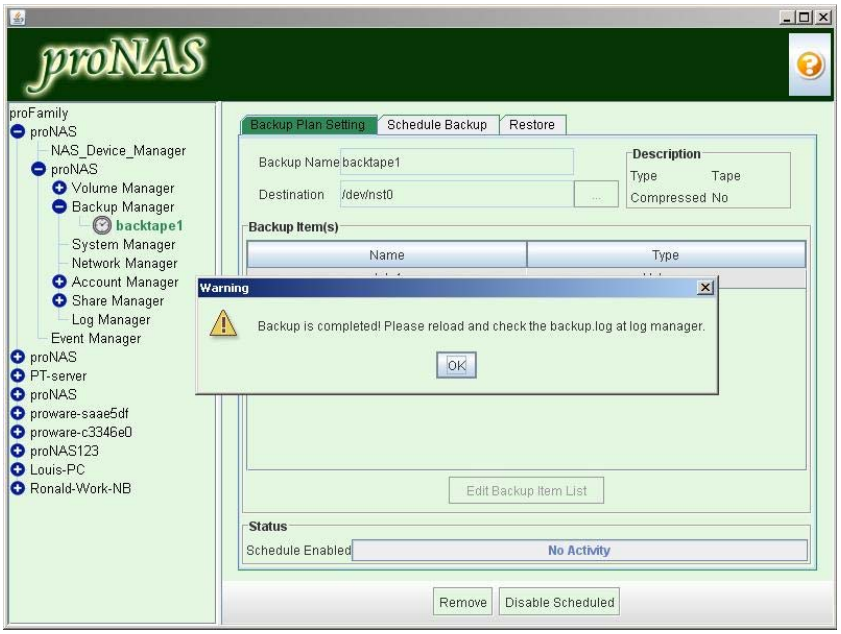
6. When the proper time comes, the scheduled backup will be executed.



7. Click “OK” to close the message. In Restore tab, check the backup name created.

8. In the succeeding days (if backup is configured for daily backup), the backup will be created automatically.



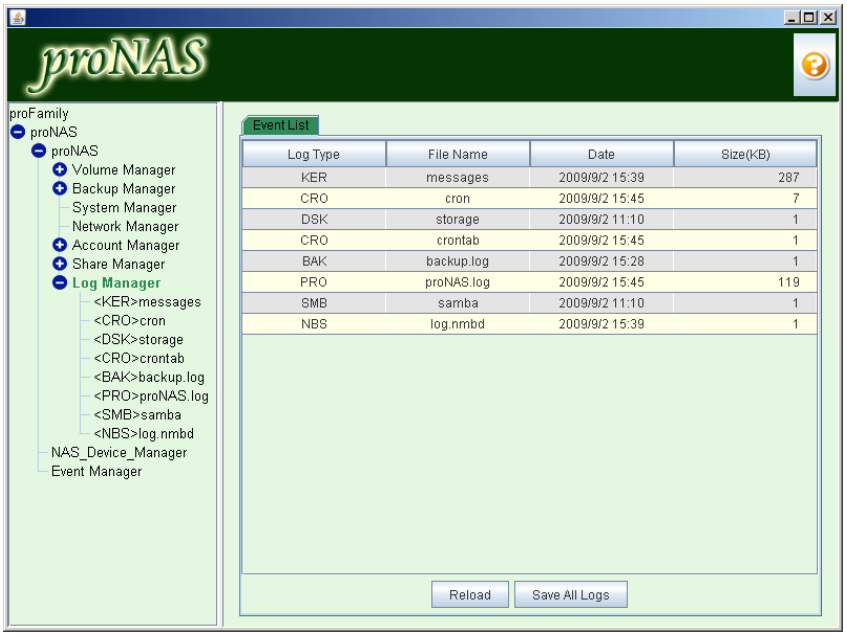


9. Verify in Restore tab the backup items that have been created.

NOTE: The procedure for restoring backup from schedule backups is the same as in manual restore. That is, select the backup name from Backup Item(s) list then click “Restore”.

8.7 Log Manager

The Log Manager enables you to view the important logs generated by proNAS.



The Event List tab of the Log Manager lists the log type, file name, date and size (KB). To update and view the latest log information, press **"Reload"**.

KER - This log contains information about the Linux Kernel service. Its path is /var/log/messages. It can store information of 7 days. This log also contains information about NFS service.

CRO cron – This log contains information about cron daemon.

DSK - This log contains information about the changes to volume. Its path is /var/log/storage.log. It can store information of 7 days.

CRO crontab – This contains Crontab information.

BAK - This log contains the status of Backup Manager.

PRO - This log contains information about proNAS service.

SMB - This log contains information about CIFS and Samba protocol. Its path is /var/log/samba.log

NBS – This log contains information about NetBIOS name server which provide NetBIOS over IP naming services to clients

RSY – This is the log for Rsync service.

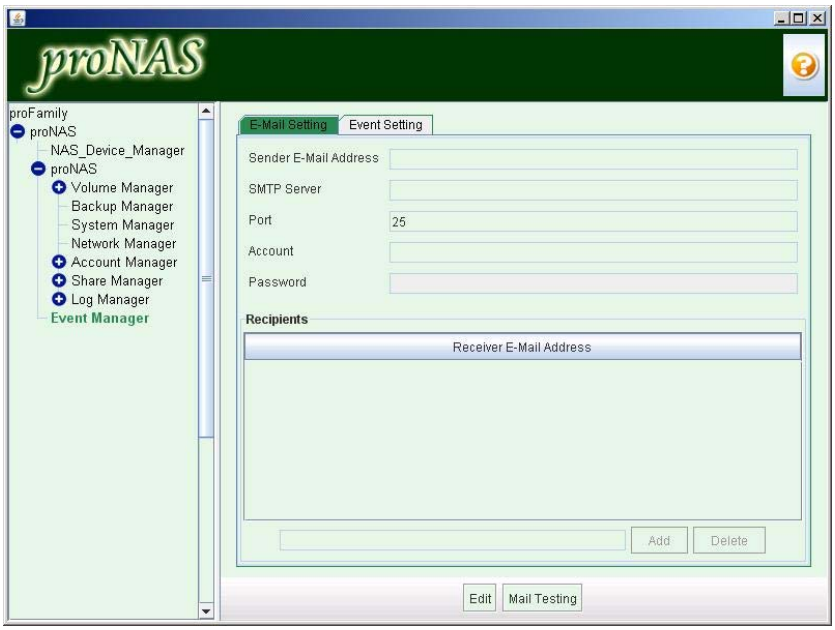
DUP - This log contains the information of the duplication function.

Save All Logs - Allows you to download all log files and save to local folder or destination.

8.8 Event Manager

Event manager is a set of management wherein you can set to receive email notifications or trigger certain commands when a **proNAS**, **proNAS HA** or **NAS Device Manager** event occurs.

8.8.1 E-mail Setting tab



Press "Edit" button to edit the following fields:

- **Sender E-mail Address** - Enter the sender's e-mail address.
- **SMTP Server** - Enter the IP address of the SMTP server.
- **Port** - Enter the port number. Default is 25.
- **Accounts** - Enter the SMTP server admin account.
- **Password** - Enter the SMTP server admin password.

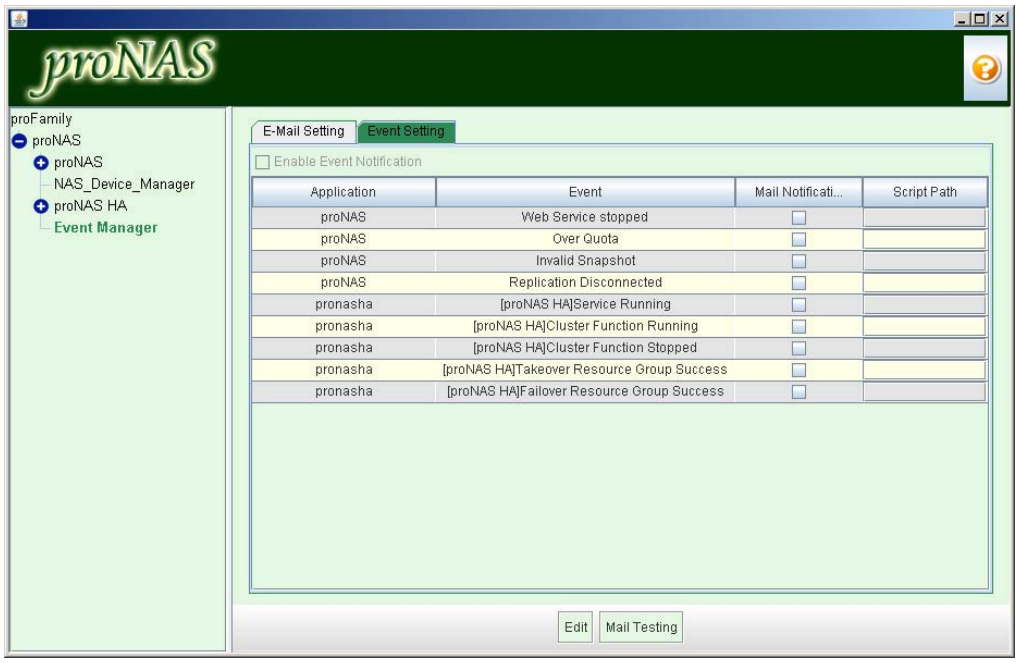
To enter a recipient's e-mail address, enter the e-mail address in the text box provided. Press "Add" button to insert the e-mail address in the Recipients list. You can have multiple recipients.

If you would like to delete a recipient, select the recipient's e-mail address and then press "Delete".

Click "Save" when done.

To verify if setting works, use the "Mail Testing" button to send a test e-mail.

8.8.2 Event Setting tab



Press "Edit" button and check the box "Enable Event Notification". Choose the following mail notification. The lists of event options will depend on which service is currently active. By default, all proNAS event will be displayed. Events for proNAS HA or NAS Device Manager will be displayed only after you have started or logon into these services.

The event options are:

Application	Event	Purpose
proNAS	Web service stopped	Notify if Apache web service is stopped.
proNAS	Over Quota	Notify if a logical volumes exceeds the given quota (full or almost full). Please check the "Send email when not enough space" for the logical volume.
proNAS	Invalid Snapshot	Notify if a snapshot became invalid.
proNAS	Replication Disconnected	Notify if replication was disconnected.
pronasha	[proNAS HA] Service Running	Notify if proNAS HA Service is running.
pronasha	[proNAS HA] Cluster Function Running	Notify if proNAS HA Cluster Function is running.
pronasha	[proNAS HA] Cluster Function Stopped	Notify if proNAS HA Cluster Function has stopped.

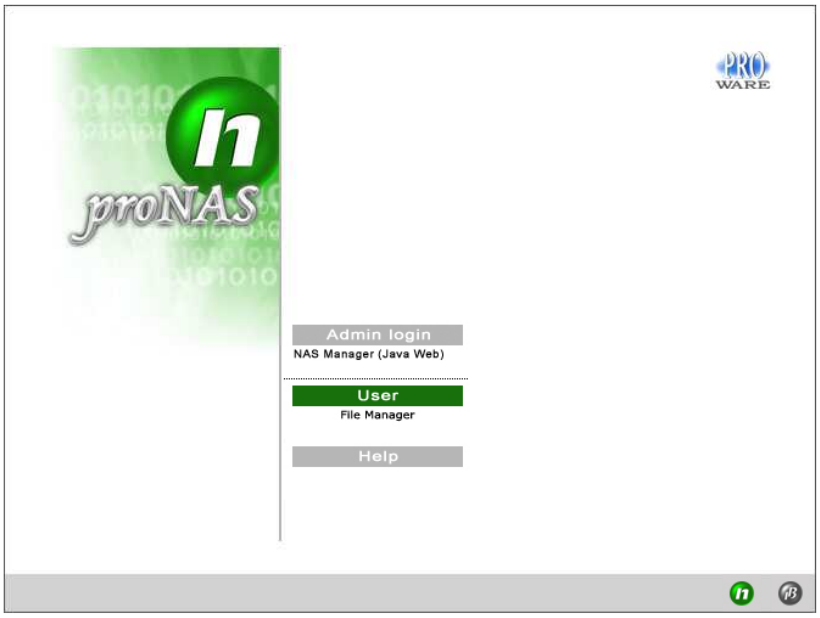
pronasha	[proNAS HA] Takeover Resource Group Success	Notify if proNAS HA Takeover of Resource Group is successful
pronasha	[proNAS HA] Failover Resource Group Success	Notify if proNAS HA Failover of Resource Group is successful

If you input a script path, please don't forget to press the Enter key after.

NOTE: The proNAS HA Application Events appear only when proNAS HA service is running.

Chapter 9 File Manager

9.1 Introduction to File Manager



File Manager is a web-base file system for normal account users to do the following actions:

Read a file: User needs the read permission of the folder and the file itself. The file may be opened immediately if the browser knows the corresponding applications that can open it, or the browser will prompt users to save the file in the local computer instead.

Upload a file: User needs the write permission of the folder and the file itself. A browser's upload window will show up and user needs to locate the file from local computer to be uploaded to the current directory.

Create a file: User needs the write permission of the folder. A browser's upload window will show up and user needs to locate the file in local computer.

Delete a file: User needs the write permission of the folder and the file itself.

Rename a file: Same as above. User needs to give the new name of a file.

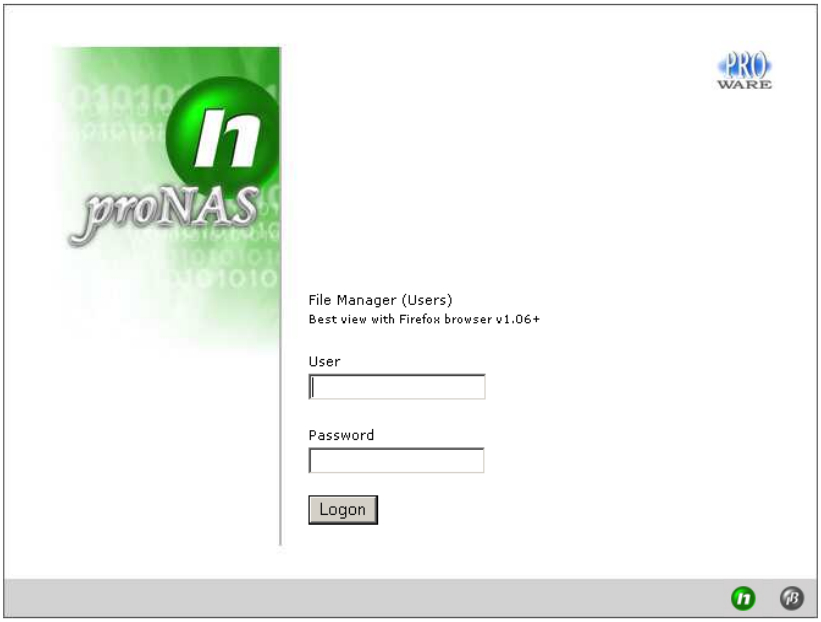
Change Password: If user needs to change password, please select this function.

Access Right (Change the ACL of a file or sub-folder): User needs to be the creator or the owner of the share folder. A user is the creator of a file or folder if user creates it. The owner of a share folder can grant the access permission of a share to other accounts or access groups. User also can manage the ACL of all the files and sub-folders under the share.

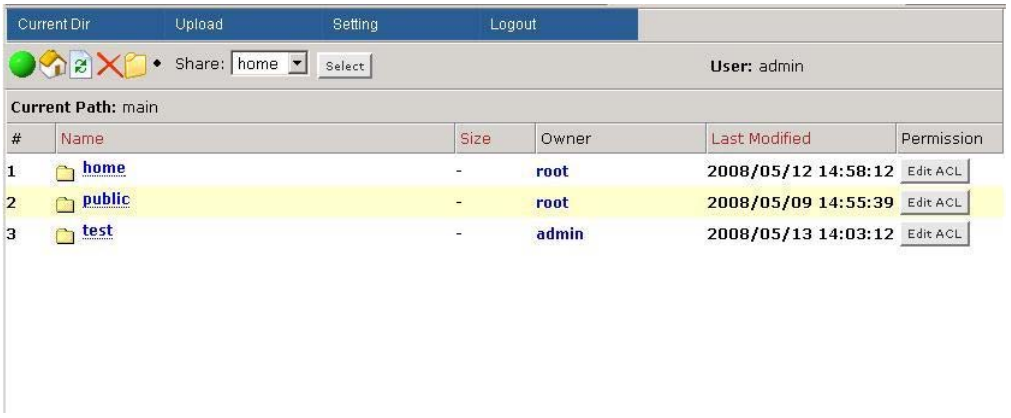
The function of access right is for share owner to do more detail management for the users accessing the shares. Share owner can increase or delete the access right of users or groups in addition to the setting of administrator in proNAS GUI. Furthermore, share owner can manage the detail access right of the subfolders.

9.2 Logon to File Manager

Enter the username and password to pass authentication.



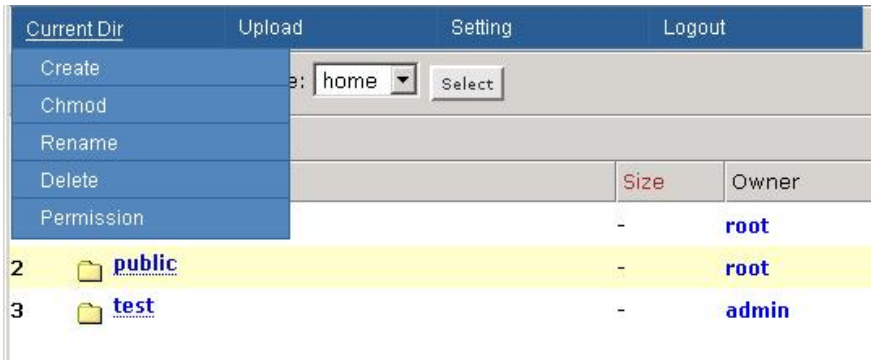
The first Screen of file Manager will display and help users to understand the possible options and to perform file management. There are 4 Main Menu in the File Manager screen: CurrentDir, Upload, Setting, and Logout. There are also short-cut icons below the main menu, like Main, Home, Reload Page, Delete Current Folder, and Create New Folder.



9.3 Directory and Upload Function

NOTE: Operations in the main Share folder, such as changing ACL or deleting the share itself, is not permitted. This must be done in Share Manager in proNAS GUI.

Current Dir – Shows possible options that can be done in the current directory.

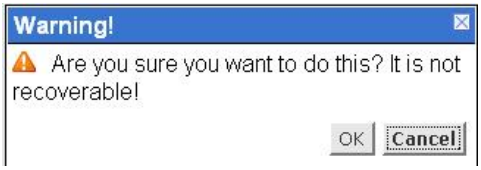


- Create – Allows user to create a new directory.

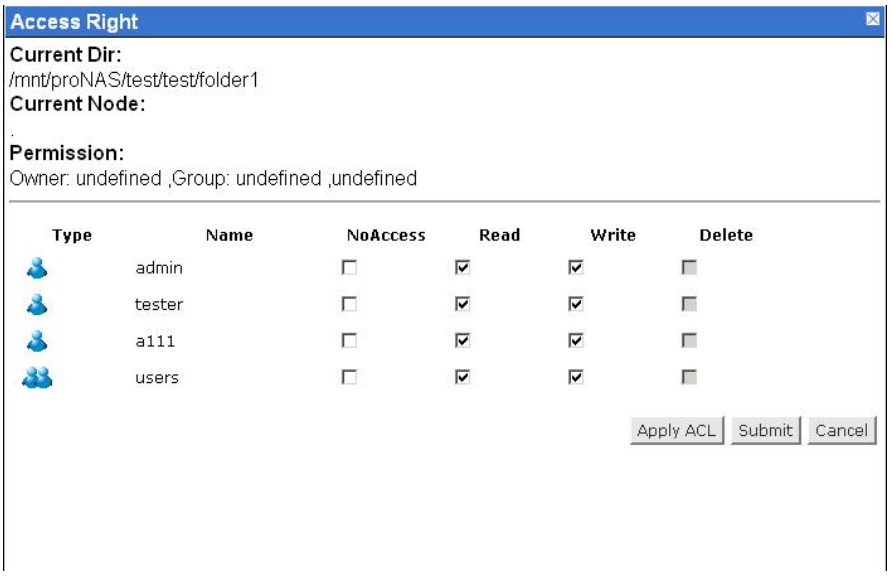
- Chmod – Allows user to change the file access permission on the current directory.

- Rename – Allows user to rename the current directory.

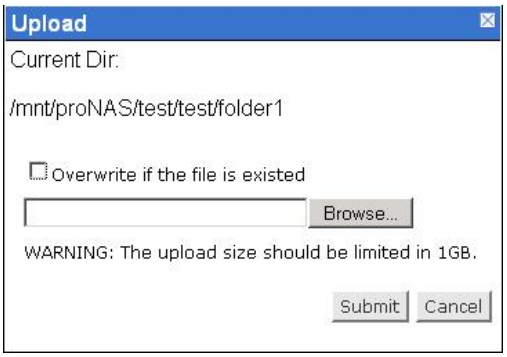
- Delete – Allows a user to delete the current directory.



- Permission – Allows user to change the Access Rights of different users on the current directory.



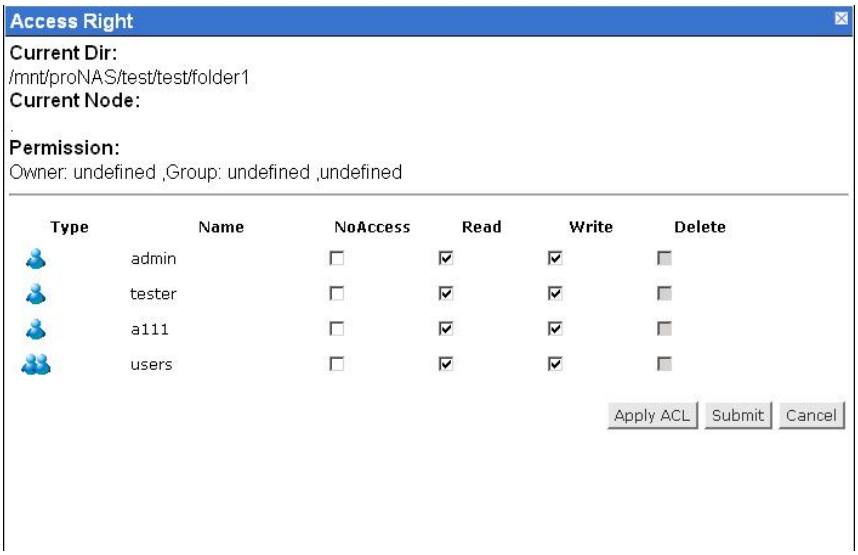
Upload – An option used to upload a local file into the current directory. Use the "Browse" button then select the file to upload.



WARNING! The file size to upload should not be greater than 1GB.

9.4 User Access Right and Group Access Right

A user who is the owner of the share can grant access permissions to other users or groups listed in the Permission list.



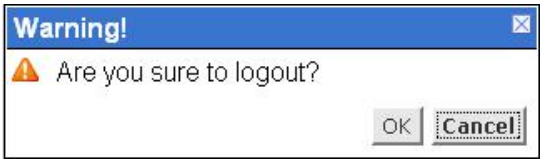
After changing the Access Rights, click the “Submit” button. The ACL will be saved and updated only in the current directory or sub-folder. To update other directories or sub-folders below the current directory, use the “Apply ACL” button. This will propagate the current ACL to the ACL off all files and sub-folders below. To cancel any changes, click the “Cancel” button.

9.5 Change Password and Logout

Setting – Allows a use to change his/her password.

NOTE: The password must be at least 6 characters in length.

Logout - Allows a user to logout from the current session of File Manager.



Chapter 10 proBackup

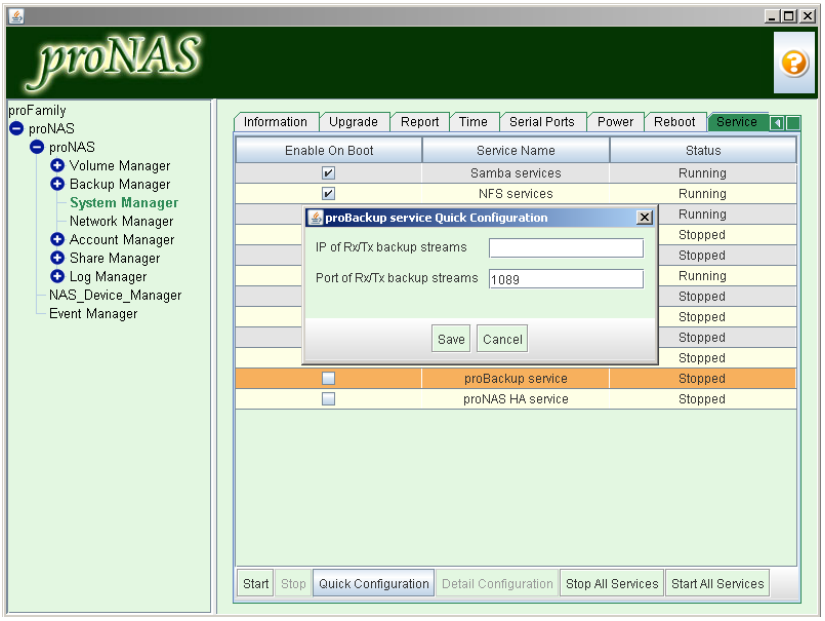
10.1 Introduction to proBackup

proBackup provides end users a friendly Java GUI that makes versatile backup functions available to general users. They can easily backup and restore their files to and from proBackup storage device, and they do not need to install proprietary software in their machines. It is also simple to setup a proBackup storage for a company or an organization, even for non-IT-pro person.

10.2 Administrator Logon

The administrator account, admin, can login to proBackup. In proNAS Manager, admin can also assign other privileged users to become member of the proBackup group. Only admin and members of the proBackup group can login to proBackup and perform proBackup functions.

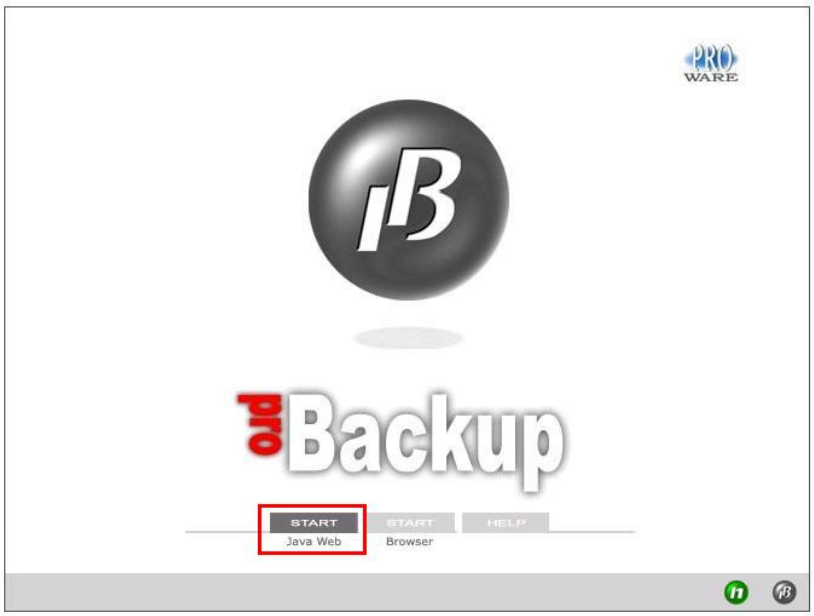
Before admin or proBackup user can login to proBackup Java GUI, the proBackup service must be started in Service tab of System Manager. In Quick Configuration, setup the "**IP of Rx/Tx backup streams**" to the **proNAS IP address** that will be used as the channel for proBackup. The "**Port of Rx/Tx backup streams**" is set to 1089 by default. If this port is already used, assign another port.



After setting the Quick Configuration options, start the proBackup service. When the proBackup service is in “Running” status, login to proBackup Java GUI can be done. The default Logical Volumes **proBackup Device** and **proBackup Extended Device** will also be created.

To login to proBackup java GUI, open web browser then type the proNAS IP address.
Click the proBackup icon on the lower right side of the page.

The proBackup page will be displayed. Click “Start Java Web”.

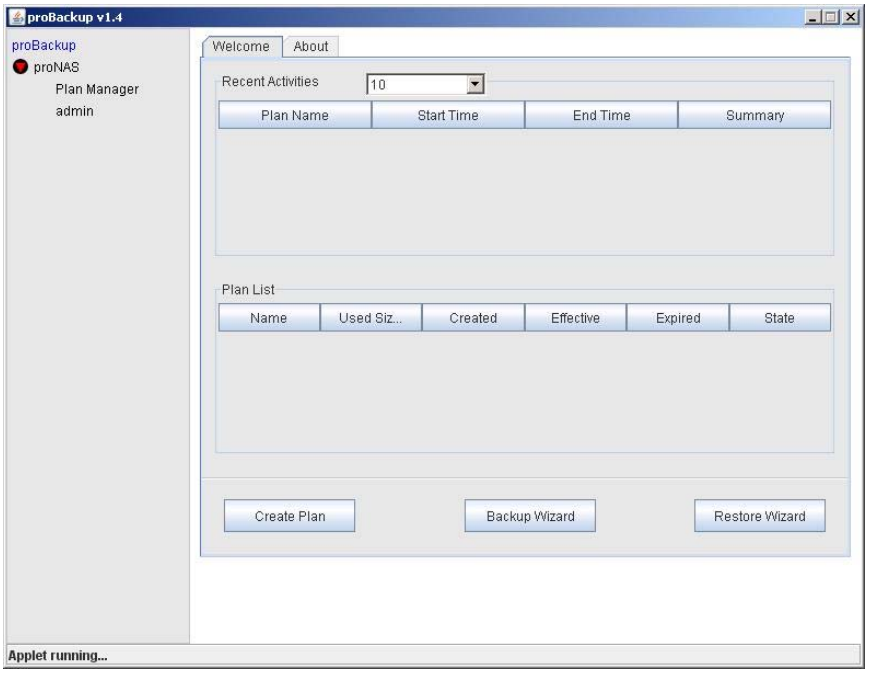


Enter the login account and password.

NOTE: All the backups of an account are lost forever if it is deleted. Please make sure of such action before doing it.

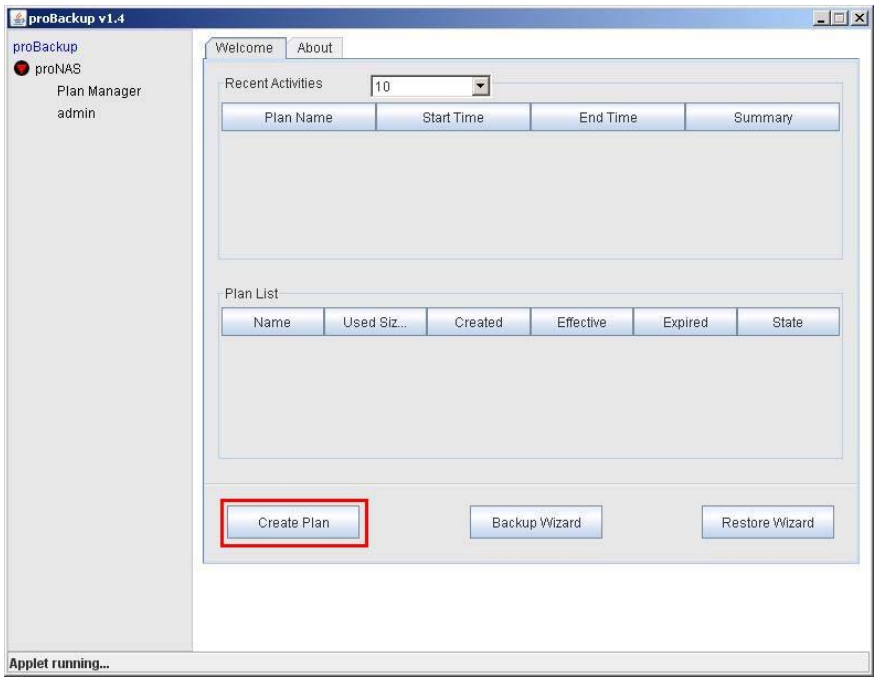
NOTE: It is advised that only the organization privilege persons can assume the role of administrator since it can restore all others' data, which may contain sensitive information.

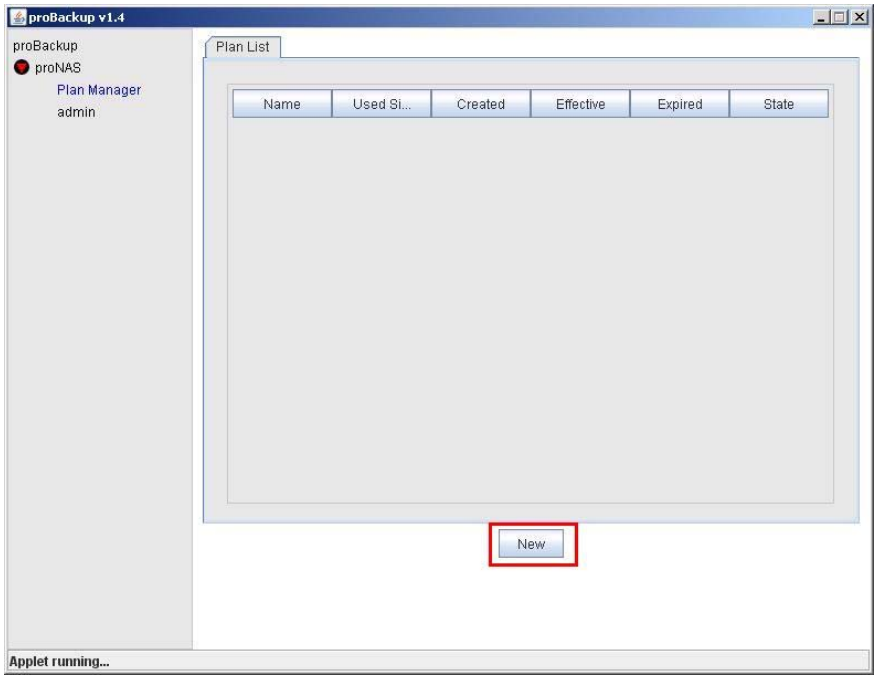
The proBackup Java GUI Welcome screen will be displayed. You can view the recent proBackup operations and existing backup plans in the Welcome screen. To learn about proBackup release version, click the About tab.



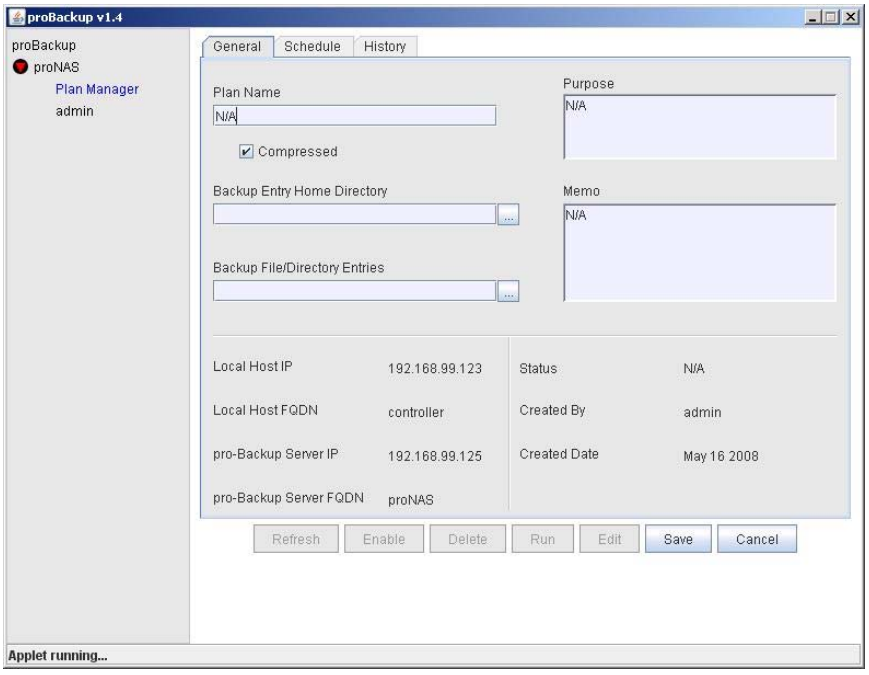
10.3 Create Backup Plan

To create backup plan, either click the “Create Plan” button in the proBackup main screen or click the “New” button in Plan Manager.



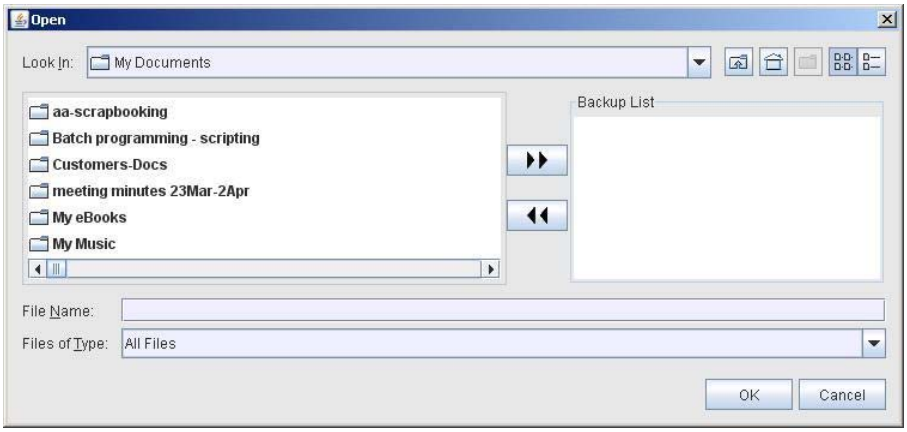


The General tab of Plan Manager will be displayed. Fill in the required fields. Some information about Local Host and proBackup Server are also shown.



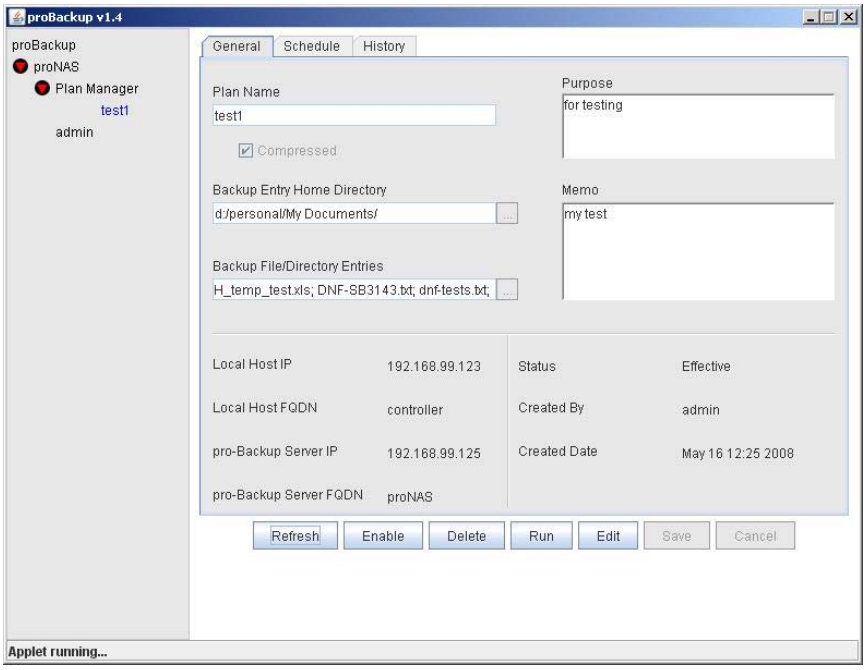
The Configuration options:

- **Plane Name** – Enter the backup plan name.
- **Compressed** – If checked, the backup will be in compressed format.
- **Backup Entry Home Directory** – Click the "…" button then select the directory when data will be backed up.
- **Backup File/Directory Entries** – Click the "…" button. Select the files and/or directories to be backed up then click ">>" button to add them to the backup list. Click "OK" to go back to General tab.



- **Purpose** – Enter additional information in this optional field.
- **Memo** – Enter additional information in this optional field.

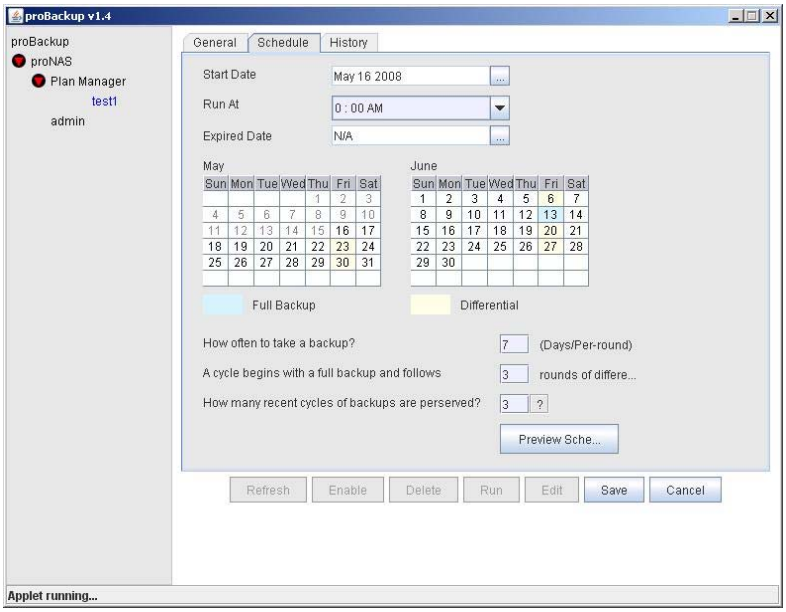
After completing the necessary information, click “Save” button. The Backup Plan will be saved.



Function buttons in the General tab.

- **Refresh** – Refresh the information about the current backup plan.
- **Enable** – Activates the backup plan schedule. When enabled, a “**Disable**” button will appear which can be used to deactivate the backup schedule.
- **Delete** – Deletes the current backup plan.
- **Run** – Execute the backup plan immediately.
- **Edit** – Use this to change settings in the backup plan.

To add schedule in the Backup Plan, click the “Edit” button then select Schedule tab. Configure the Schedule options then click “Save” when done.



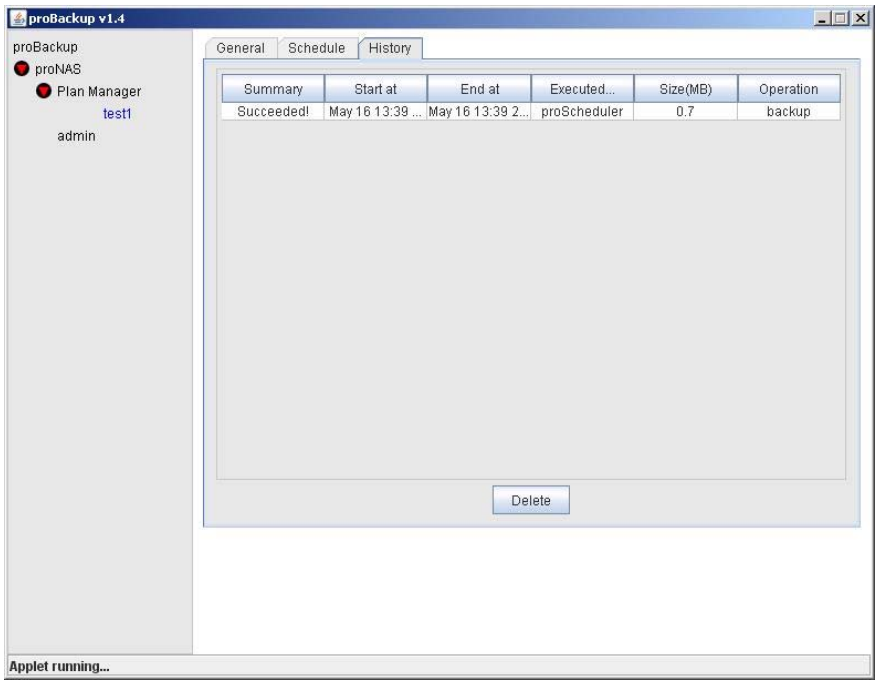
Schedule options:

- **Start Date** – The starting date when the backup will be done. This usually defaults to the current date. Click the “…” button. A calendar will be displayed. To change the Start Date, select a new date in the calendar.
- **Run At** – The preferred time to run the backup. To change the Run At time, click the pull-down arrow then select the preferred time.
- **Expired Date** – The ending date for the backup. To change the Expired Date, click the “…” button then select in the calendar the preferred last date of backup.
- **How often to take a backup? (Days/Round)** – The number of days that will pass before a differential backup will be done.
- **A cycle begins with a full backup and follows rounds of differential backup** – Enter the number of differential backups that will be made before starting a new full backup.
- **How many recent cycles of backups are preserved?** – Enter a number which is the total number of backup cycles that will be preserved. A backup cycle starts with a full backup and ends with the last differential backup before the next full backup. When the number of cycles in a schedule has been reached and a new cycle is started, the oldest backup cycle will be automatically removed.
- **Preview Schedule** – Click this button to update the calendar schedule.

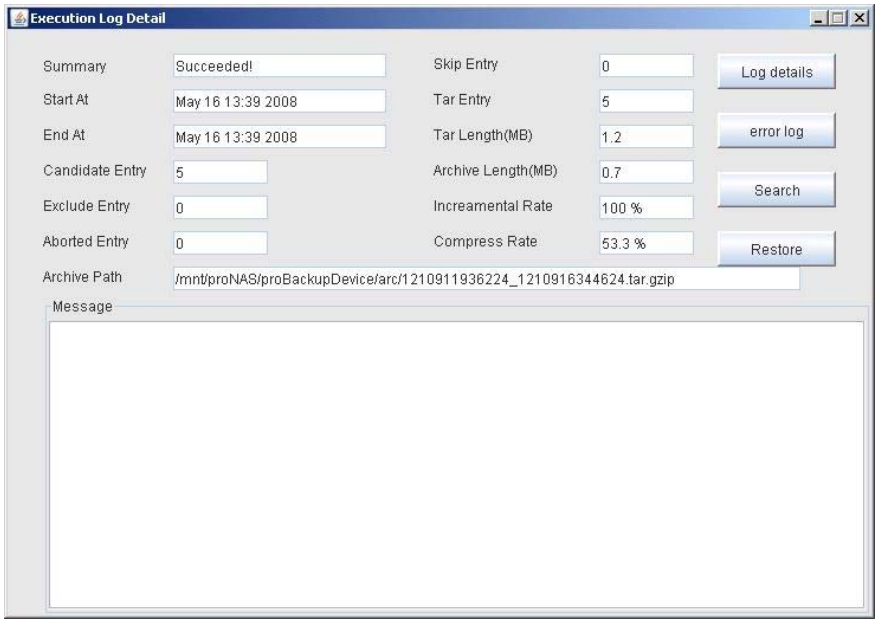
    - **Full Backup** – archival backup; all files are copied to a backup storage device
    - **Differential Backup** – backup only the data files that have been modified since the last full backup

Click “Save” to update the schedule settings. Then click “Enable” to activate the backup schedule.

The History tab shows a log or list of operations that have happened in proBackup such as backup or restore operation. To delete an entry in the history list, select the item in the list and click “Delete”.

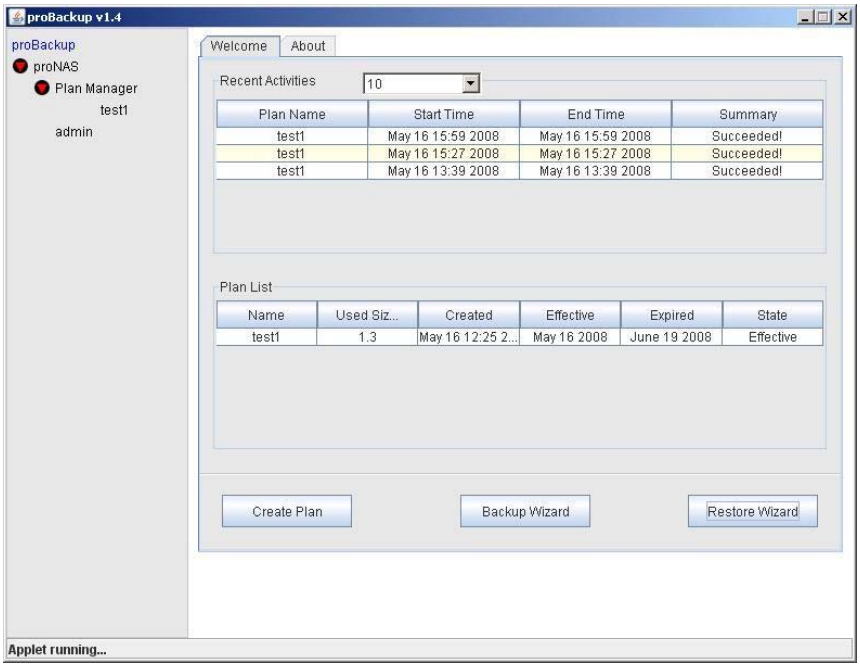


To view detailed information about the backup, double-click the item from the History tab.



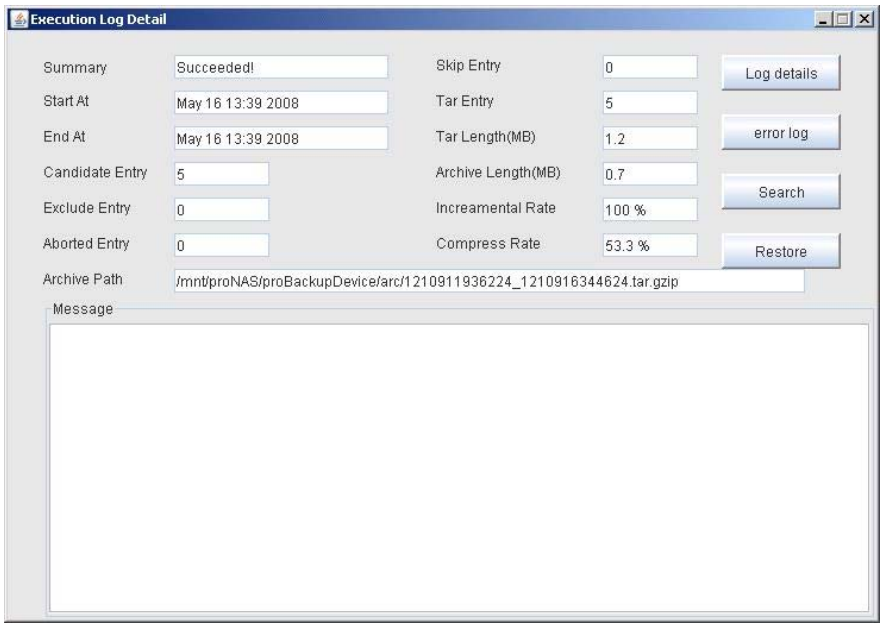
“Log details” is used to display detailed information about the execution process.
“Error log” will display errors that happened during the execution process.
“Search” will allow you to search for a string currently displayed in the Message screen.
“Restore” will allow you to restore a backup.

Another alternative to do backup or restore is to use the Backup Wizard and the Restore Wizard. Click proBackup in the left tree node. The Welcome screen will be displayed where the Backup Wizard and Restore Wizard can be used.



10.4 Restore Backup

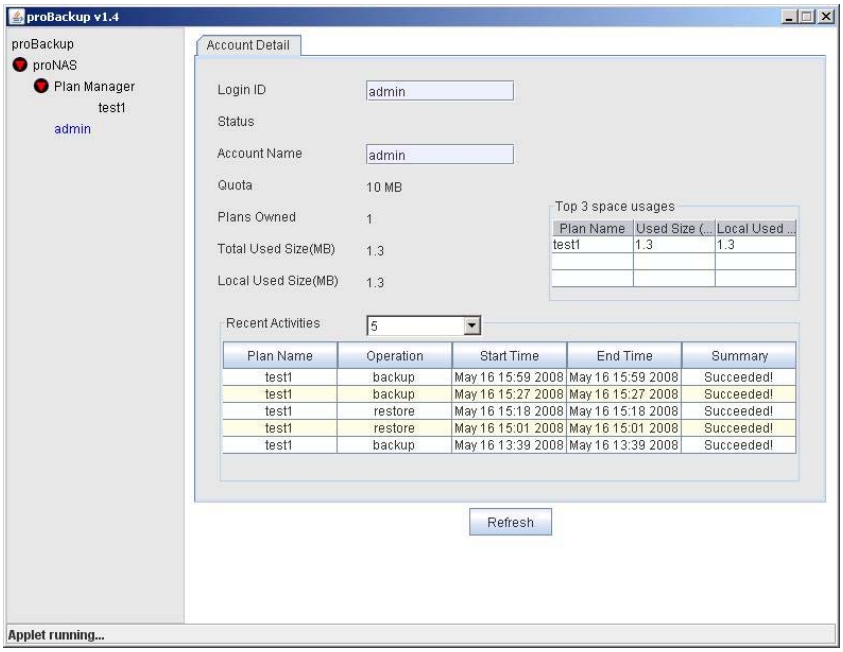
To restore a backup, double-click the backup item from the History tab. The Execution Log Detail window will appear.



Click “Restore”. Then input the destination where the data will be restored. Or click the “Browse” button then select the destination directory or folder where data will be restored. Click “Ok” to start the restore process.

10.5 Account Detail

Under Plan Manager, click the account name to view information about the account.



Chapter 11 proNAS HA (Optional Function)

11.1 Introduction to proNAS HA

proNAS HA (High Availability) provides solution for business continuity with automatic failover which ensures that should a critical server become unavailable - due to failure or maintenance-related downtime — a replica will immediately provide all services in its place without the need for time-consuming manual procedures.

The core processes of ProNAS HA are implemented as two mutual-guarded fail-safe proNAS services. They can be manipulated by accessing the Services tab in the proNAS System Manager node. The dual service architecture of ProNAS HA prevents ProNAS HA from being the single-point-of-failure of the server cluster.

When a server is down or unavailable, ProNAS HA switches the critical operations of that server over to the peer server automatically. The switch over procedure can also be triggered manually to handle scheduled downtime more gracefully and user transparently. ProNAS HA can be manually instructed to switch over the critical operations of a server to the peer server. Users can then perform upgrade, replacement, or maintenance to the hardware and software of that proNAS server. The critical operations of a server can be configured as auto-switch back. After those critical operations were taken over by the peer server, ProNAS HA can switch them back to their original active server when the active server becomes available again. Auto-switch back ensures that the original load distribution between the two servers will be resumed immediately when possible.

proNAS HA provides:

- Manual or auto-triggered failover to a standby server.
- Supports manual or automatic failover back to the original server when ready
- Real-time replication minimizes potential data loss

NOTE: proNAS version 1.3.xx supports Replication of Logical Volumes with LV capacity up to 16TB. proNAS HA also has the same LV size limit, which means all logical volumes in proNAS (under HA) must not exceed 16TB.

11.2 Getting Started with proNAS HA

Before Configuring High Availability

Before attempting to configure two proNAS servers as a High Availability pair, check the following requirements:

1. **Each proNAS server node must have a different and unique hostname. (It is highly recommended to use the same NAS model.)**
2. **Each proNAS node must have at least two static IP addresses.**
3. **Must have a reliable heartbeat, private net Ethernet is required, serial RS232 is optional.**
4. **ProNAS HA services must be started in both proNAS servers.**
5. **The maximum number of logical volumes that can be created under HA is 32.**
6. **ProNAS HA does not support logical volumes larger than 16TB. Users can create and extend volumes larger than 16TB but this cannot be used in proNAS HA.**
7. **Changing hostname and IP addresses when proNAS HA is running is not allowed.**
8. **Snapshot function is disabled under HA.**
9. **Be sure there are no scheduled snapshot task enabled either on each proNAS box.**
10. **ProNAS HA service cannot be started if iSCSI volume exists, Replication is running, or snapshots exist. Make sure to remove all iSCSI volumes, stop Replication, or delete snapshots.**

Setting up a private network:

Private net is a communication channel between the two proNAS box through which they exchange information about their states (*heartbeats*). proNAS supports two private network, TCP/IP Socket and RS232 Serial Port.
To setup TCP/IP private net: Connect a dedicated network into Ethernet1 adapter. You may use a crossover cable. Ethernet0 serves as your public net.
To setup RS232 Serial Port private net: Connect a serial cable to either Com1 or Com2 of both proNAS nodes then configure it under the "Serial Port" tab on System Manager.

NOTE: It is recommended to use both TCP/IP and RS-232 for your private net. Private net IP will be used for replication and RS-232 for heartbeat.

NOTE: You can setup LAN0 Gigabit port (eth0) as your public net; that is where the users access your proNAS, and also for accessing proNAS management GUI. Then use LAN1 (eth1) as your Private Net.

11.2.1 Hardware Aspect

Active server: proNAS HA server that performs cluster-protected operations.

Backup (Standby) server: proNAS HA server that can takeover the critical operations of an active server when the active server is down or unavailable.

Private net: Private net is a dedicated channel for servers to exchange their operating status (i.e., heartbeat message).

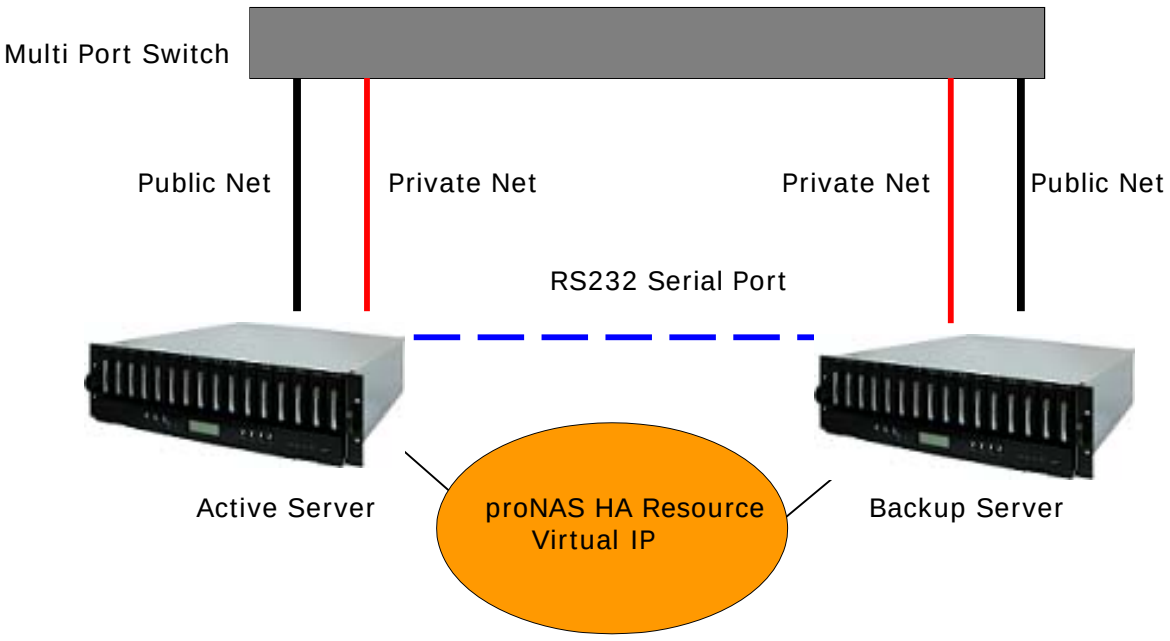
Types of Private Net Available:

- **TCP / IP socket:** Ethernet network running TCP/IP protocol. Each server must install a dedicated IP to attach to the private net.
- **RS-232 serial port:** One free serial port per server. A null modem cable must be installed to connect the serial ports of the two servers.

Public net: Public net is the paths for networked clients to access cluster- protected resources.

Network Configuration for High Availability Pair

The following diagram illustrates the network configuration for a High Availability pair:



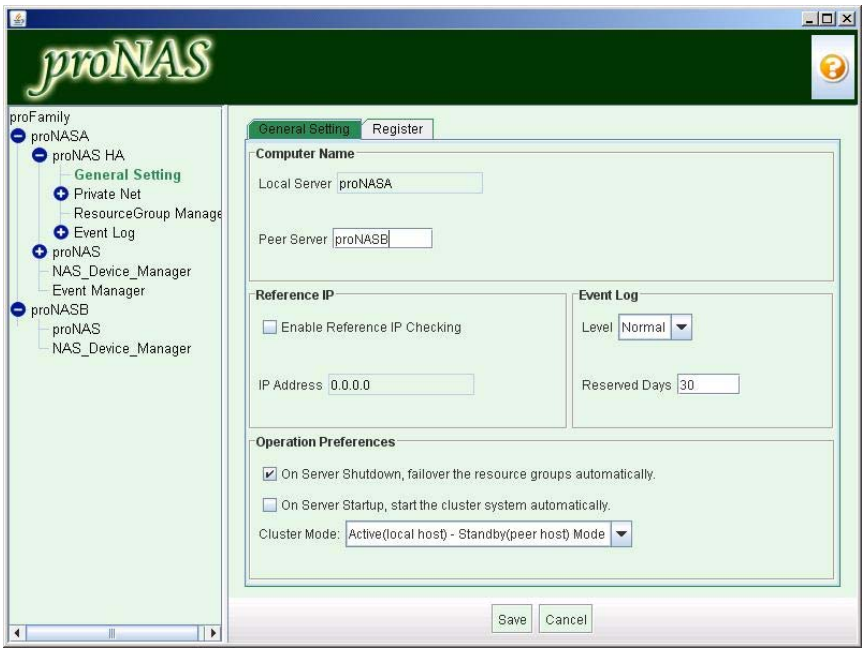
11.2.2 Procedure for Setting Up proNAS HA

Setting up a server cluster:

Below are the basic steps in setting up a server cluster:

1. Configure the hostname for both proNAS servers (must be unique).
2. Configure two static IP addresses for each proNAS server.
3. Set up private net. At least the private net IP must be configured to start cluster.
4. Start proNAS HA service for both proNAS servers. Select System Manager, and then Services tab, and highlight proNAS HA service then click Start. proNAS HA node will then appear on the left tree after the service starts successfully.
5. On the designated Active Server, go to proNAS HA->"General Settings".
6. On the "General Setting" tab, click "Edit" button. Input the Peer Server hostname then select "**Active(local-host) – Standby(peer host) Mode**" under the Cluster mode. Click "Save".

NOTE: The Cluster Mode of Backup Server must be configured as "Standby(local host) – Active(peer-host) Mode" (see Step 10).



Other configuration options:

Computer Name:

Local Server: The hostname of the Active or Primary server
Peer Server: The hostname of the Backup or Secondary server

Reference IP:

Enable Reference IP Checking – Select this option to enable reference IP checking. A Reference IP is an IP address that the proNAS HA service will check when the heartbeat channel(s) between the two servers are lost. This IP will be used as a reference point to device whether the network really has a problem before doing failover or takeover. HA will ping the local and virtual IP address of proNAS, and for any reason that this fails, HA will ping this reference IP as a double check. If ping still fails, proNAS HA will proceed with failover or takeover. The IP of a router or any network device which is always online can be used as a Reference IP.

IP Address – Enter the IP address of the Reference IP to check the availability of the servers.

Event Log:

Level – Select the type of logging that will be used for proNAS HA service. Default is Normal which shows operation processes. Other option is Trace, which shows operation and traceable processes.

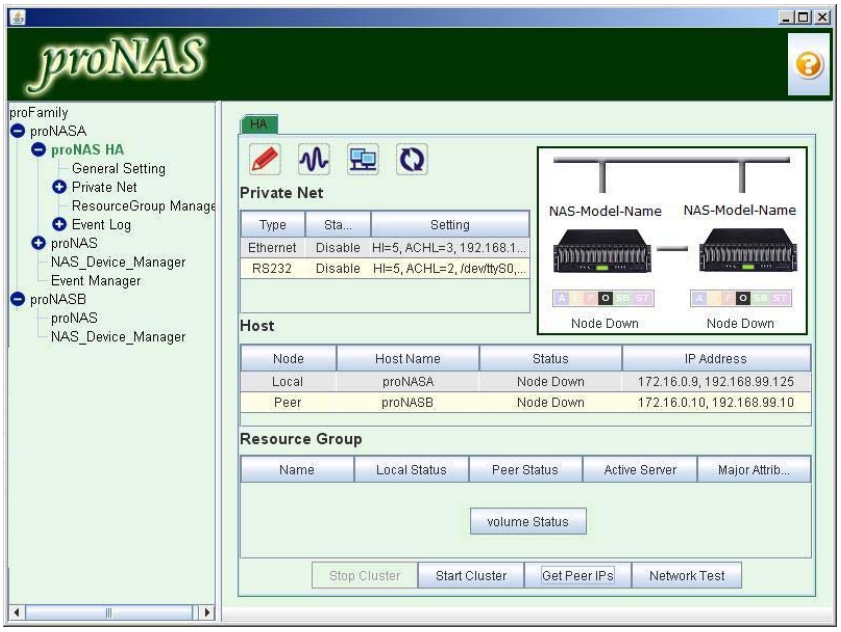
Preserved Days – Select the number of days that the log will be preserved before deleting.

Operational Preferences:

On Server Shutdown, failover the resource groups automatically – When enabled, the resource groups will be failed over to the other server when this server shutdown.

On Server Startup, start the cluster system automatically – When enabled, the cluster system will be started automatically when this server starts up.

7. Back to proNAS HA node, click "Get Peer IPs" button. The IP addresses of the peer server will then be displayed in the status info table. Be sure that it gets the peer IP addresses! If it fails, check again the hostname that you supplied in step 6.

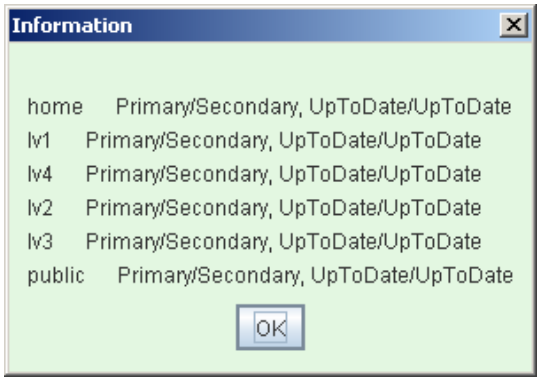


Buttons:

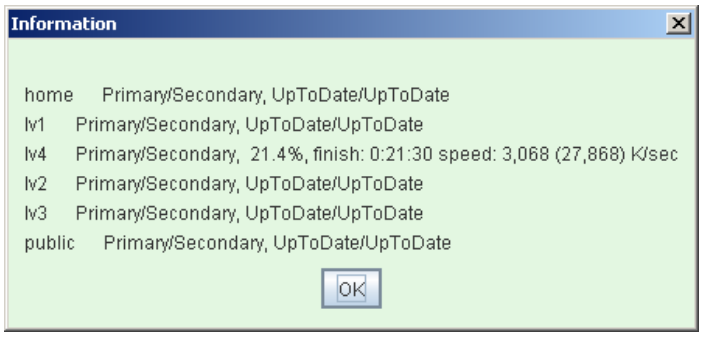
Stop Cluster	Stop Cluster Operation.
Start Cluster	Start Cluster Operation.
Get peer IPs	Get the IP's of the peer server and display it in the host peer table.
Network Test	Tool for testing network IP address (e.g ping ip)
Volume Status	Shows the current Replication status of logical volumes.

NOTE: When HA is already configured and Cluster is in operation, you can see the current replication status of logical volumes by clicking "Volume Status".

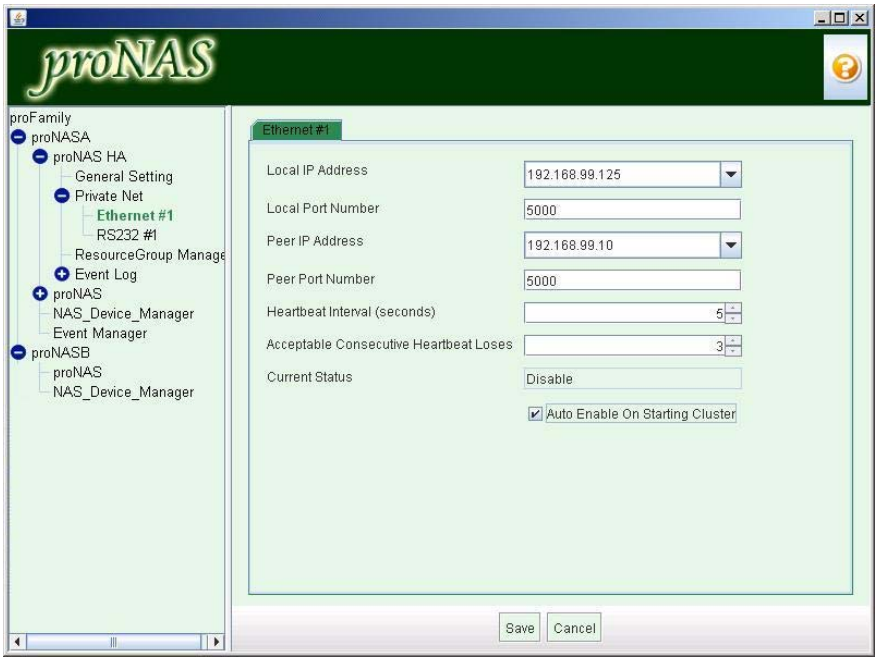
Volume Status Example 1: All logical volume Replications are up to date.



Volume Status Example 2: Replication of one logical volume is initializing.



8. Go to Private Net node down to "Ethernet#1". Set the local and peer IP address, check "Auto Enable on Starting Cluster" then save. Be sure not to select the public IP (eth0 IP address) for both proNAS servers.



Private Net: Ethernet

Local/peer Port Number	Specify an unused TCP port for each server to receive the heartbeat sent from the peer server. The default value is 5000.
Local/peer IP Address	Specify the IP Addresses of the network interface cards that constitutes both ends of the private net. These IP addresses must be on a separate subnet from the public net.
Heartbeat Interval	Specify the period of time between two consecutive heartbeats.
Acceptable Consecutive	Each server will keep counting and timing the heartbeats received from the peer server. If the number of times a

Heartbeat Loses	server fail to receive the heartbeat in time exceed this threshold, the peer server will be considered down or unavailable. The resource group of the peer server will be taken over.
Auto enable on starting cluster	This option is disabled by default. This private net will be enabled automatically when starting cluster. Add the checkmark to enable this option.

9. Configure private net "RS232#1", if you setup serial port as an additional private net.

Private Net: RS232

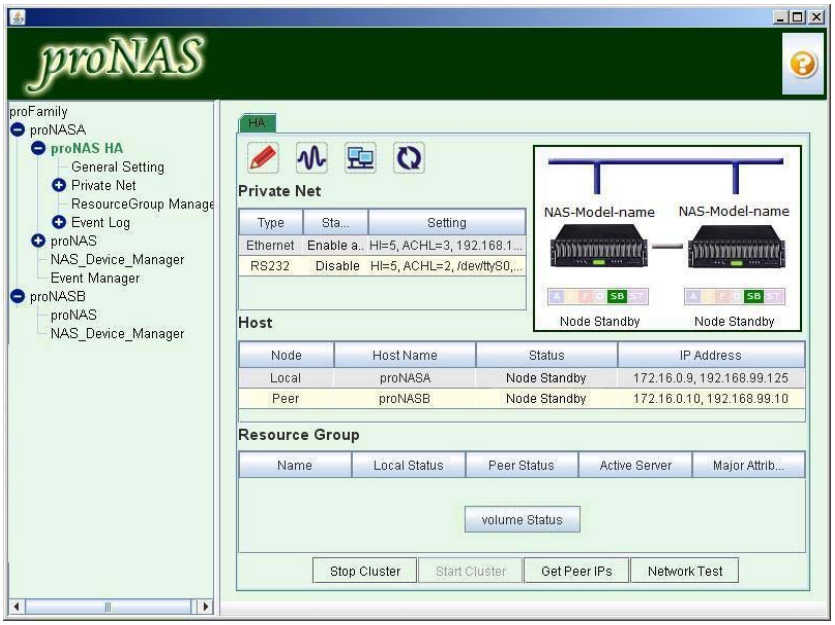
To use RS232 as a private net, you need to configure Serial ports settings in proNAS System Manager > Serial Ports tab, select either COM1 or COM2 for proNAS-HA.

Local Serial Port	Specify an unused serial port for each server to receive the heartbeat sent from the peer server.
Baud Rate	Specify the Baud Rate of the selected serial ports.
Heartbeat Interval	Specify the period of time between two consecutive heartbeats.
Acceptable Consecutive Heartbeat Loses	Each server will keep counting and timing the heartbeats received from the peer server. If the numbers of times a server fail to receive the heartbeat in time exceed this threshold, the peer server will be considered down or unavailable. The resource groups of the peer server will be taken over.
Auto enable on starting cluster	This option is disabled by default. This private net will be enabled automatically on starting cluster. Users can add the checkmark to enable this option

10. Follow the same steps from step 5 to step 9 to configure your standby Backup Server except you need to select "**Standby(local host) – Active(peer-host) Mode**" as the Cluster Mode.

11. Click "Start Cluster" button.

12. Wait until the status of the local and peer server are in be standby-standby mode respectively. The statuses of the private net must also be "Enabled and Healthy". If this is not the output, check and repeat previous steps.



13. Go to "Resource Group Manager" then press "Add Resource Group".

The Resource Group Manager of proNAS HA is used to manage resource groups. Users need to configure resource groups only on one of the servers, usually the Active server. proNAS HA will automatically synchronize the status of resource groups between both servers. Note that users are prohibited to create or remove resource groups unless proNAS HA are running on both servers and at least one of the private net is functioning.

Buttons:

Add Resource Group button	Add new resource group member. User can specify the name of the resource group. This name must be unique for the resource groups within the cluster
Switch All Resource Groups from Peer	This is to manually takeover the all resource groups from the peer server. Users can manually takeover resource groups from the peer server to perform maintenance or troubleshooting on the active server. This button will be displayed only if resource groups are bring in.
Switch All Resource Groups to Peer	This is to manually failover the all resource groups to the peer server. Users can manually failover resource groups to the peer server to perform maintenance or troubleshooting on the active server. This button will be displayed only if resource groups are bring in.

14. Input a resource group name. You may check "Auto Switch back" or "Auto Bring In" then click “Save”.

Resource Group Properties:

Resource Name	A unique name for identifying the resource group
Active Server	The active server of the resource group
Backup Server	The peer server is automatically display
Local Status	The status of the local server
Peer Status	The status of the peer server
Auto-switch back	An option for enabling the Group to be switched back from the Backup server to the Target server automatically when the Target Server is available again.
Auto Bring In	An option for enabling the resource group to be brought in automatically when Cluster is started.

Buttons:

Bring in	The selected resource group will be activated and brought under the protection of proNAS HA. This button is only visible if there are resource group added.
Bring out	The selected resource group will be brought out from the protection of proNAS HA. A resource group can be brought out of cluster to perform maintenance or troubleshooting. This button is visible if resource groups are brought in.

15. Click the resource group name on the left tree node then press "Add Resource".

16. On the "Basic Settings" tab, input a resource name.

Resource Basic Setting:

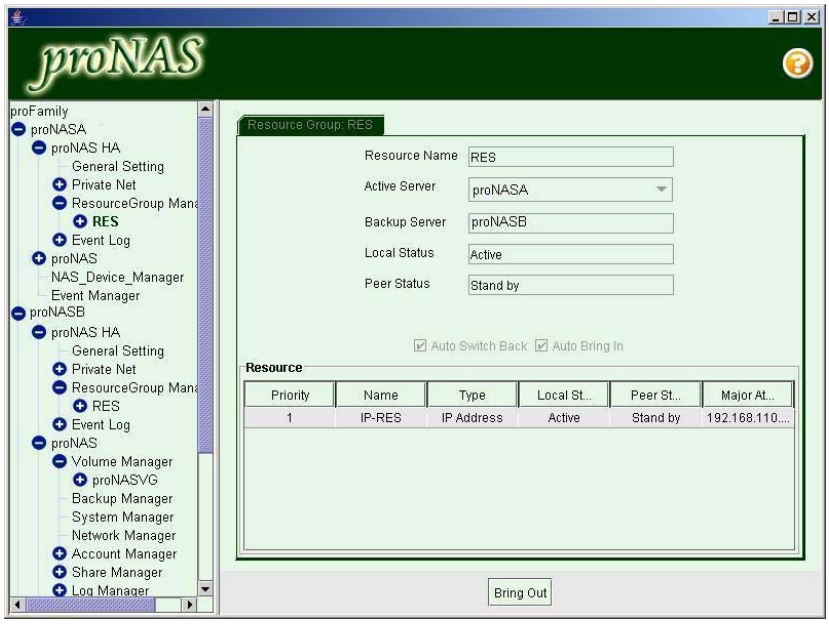
Resource Name	A unique name for identifying the resource group.
AC interval (Availability Check Interval)	A time interval for proNAS HA to check the availability of the resource group periodically.
AC Retry (Availability Check Retry)	The number of times for proNAS HA to check the availability of the resource group periodically.
Stop timeout	Specify the period of time for resource startup and stop. If a server fail to receive the heartbeat in time exceed this threshold, the peer server will be considered down or unavailable. The resource group of the peer server will be taken over.
Skippable if releasing resource fail	This option is disabled by default. Basically all of the resource group of the peer server will be taken over when the peer server fails. Users can add the checkmark to enable this option. The failover will be taken even if resource releases fail.

17. On the "IP Address Resource" tab, select the original IP address (eth0 IP) for both local and remote proNAS, enter an active IP address, active subnet mask and then save. Active IP address is the virtual IP address.

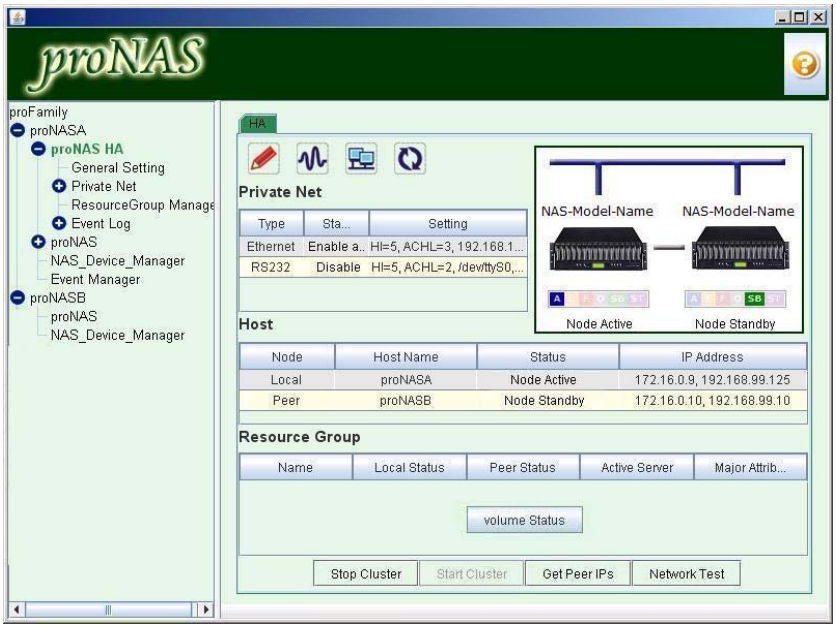
IP Resource:

Original IP Address	Choose the original IP Address for the local and peer server.
Active IP Address	Type an IP Address (virtual IP) for client-end applications to access specific resources on the NAS Target Server.
Active Subnet Mask	The subnet mask used by the Active IP Address.

18. Click the resource group name on the left tree node then press "Bring In". The resource name will be brought in.

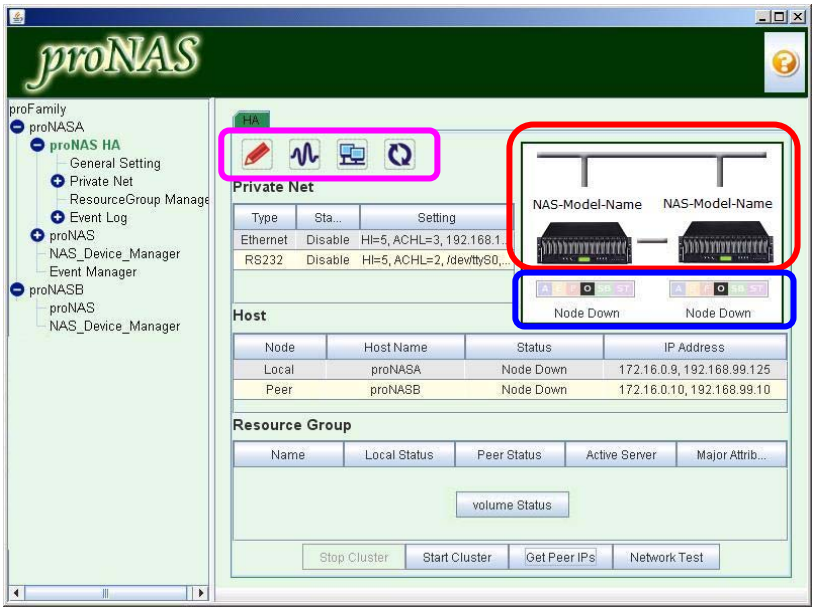


19. The Cluster Servers will be in Active – Standby mode.



11.3 ProNAS HA Properties

Status Properties



Users can monitor all the resources from the proNAS HA Status Pad. Users can monitor the status of the servers, the resource groups and the private net in real-time. The status after the Cluster Service starts running on both servers.

The status icons in status bar and their respective meaning:

- Active Mode

- Error Mode

- Fail Mode

- Offline Mode

- Standby Mode

- Startup Mode

The private net status:

The colored lines between the servers indicate the status of the private net. Also status is displayed in the function bar.

- **Gray line** Only one end of the Private Net is created, the other end is not yet created.
- **Red line** Both ends of the Private Net are established but either one of the servers can not receive heartbeat message from the peer server.
- **Blue line** Both ends of the Private Net are established and both servers are exchanging heartbeat messages.

Indicators:

Users can accurately monitor the status of the system such as the License status, Private Net, Public Net and the resource takeover/failover. When a condition occurs, the icon will turn red. You will also see a message appear in the Event Log.

Private Net: This icon will turn red if there's a problem with the connection of the private net.

Public Net: This icon will turn red if there's a problem with the connection of the public net.

Failover/Takeover: This icon will turn red during the failover or takeover scenario.

License: This icon will turn red if proNAS HA is not registered.

Host box: Display the status of Local and Peer Server

Resource Group box: Display the resource group status

Buttons:

Stop Cluster button	Stop Cluster Operation.
Start Cluster button	Start Cluster Operation.
Get peer IPs button	Get the IP's of the peer server and display it in the host peer table.
Network test button	Tool for testing network IP address (e.g ping ip)

11.4 Extending a Logical Volume in HA

Extending a logical volume while in cluster is basically not allowed same as in replication, however here is the workaround.

1. Stop Cluster
2. Stop HA service for both proNAS.
3. Abort the replication of the logical volume that needs to be extended.
4. Extend the logical volume on the Active server.
5. Removed the logical volume (the replica) on the standby server.
6. Start HA service for both proNAS.
7. Start cluster.

NOTE: The extended LV size must not exceed 16TB.

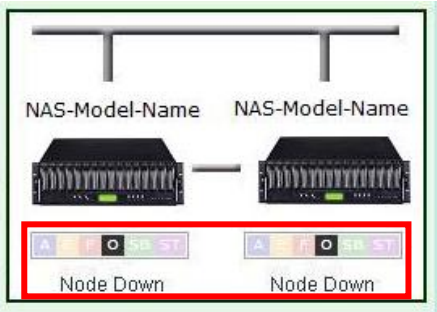
11.5 Clear All HA Configuration

A function button “Clear All HA Configuration” is provided to remove all proNAS HA configuration. This is located in General Setting tab.

When you clear the HA configuration, you have an option to clear all logical volume Replication. If you don’t clear the all Replication, only HA configuration will be reset, and all logical volumes will still have Replication.

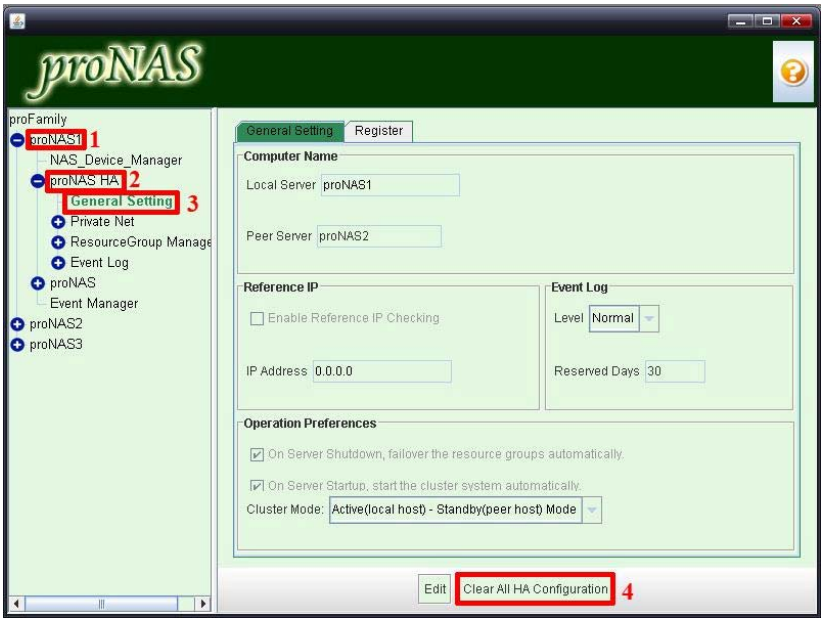
After you clear all HA configuration and clear all Replication, you can re-configure another HA. This is normally used when one of the proNAS servers has failed and you want to reconfigure HA for another (new) proNAS server using the remaining proNAS server.

IMPORTANT: Before you clear all HA configuration, make sure the cluster is stopped (all nodes are “down”).

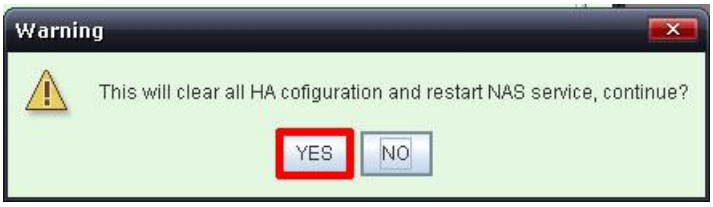


To remove all existing proNAS HA configuration:

1. Select the proNAS node name, click proNAS HA, and select General Setting. Click “Clear All HA Configuration”.



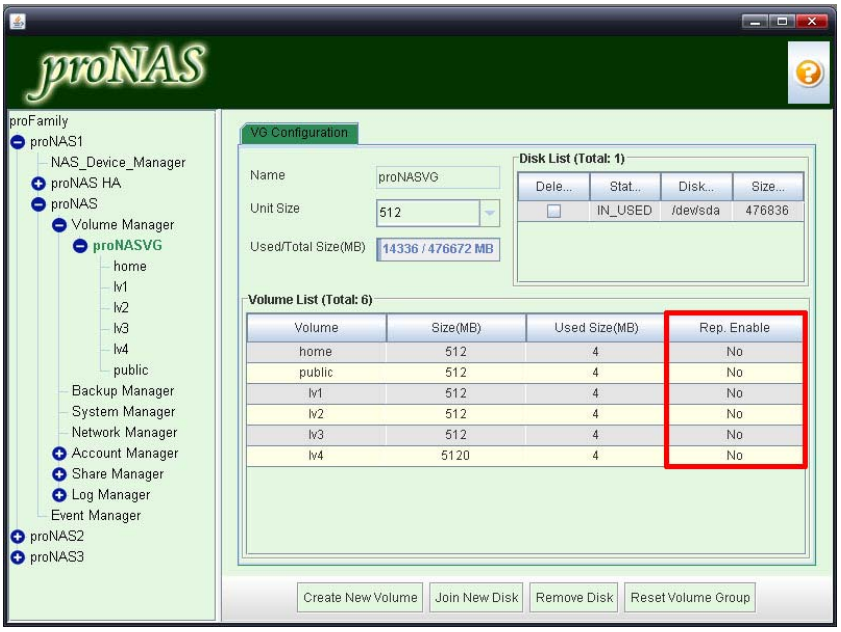
2. A warning message to clear all HA configuration will be displayed. Click “Yes” to proceed.



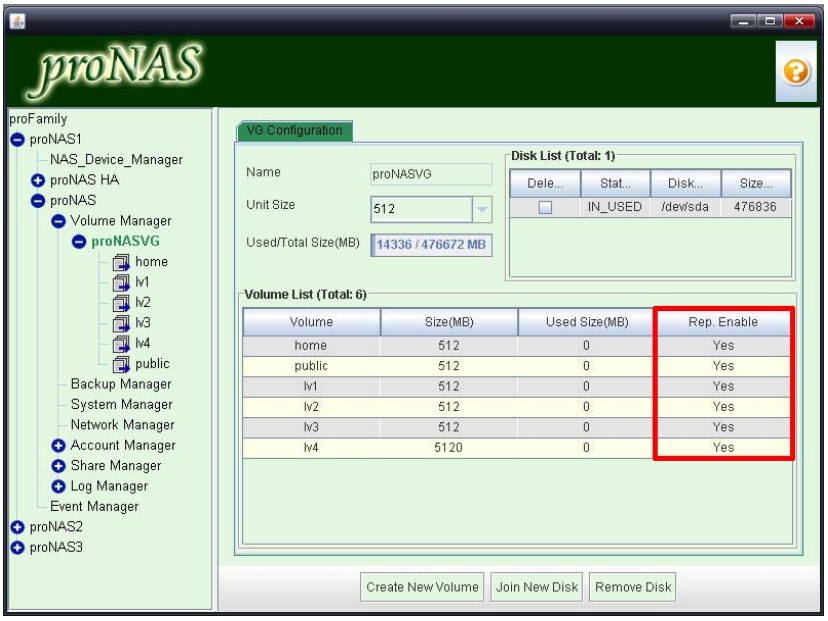
3. A warning message to remove all replication in logical volumes will be displayed. Click “Yes” to remove Replication in all logical volumes, or “No” to just clear HA but replication of logical volumes still exists.

4. An information message will be displayed. Click “OK” to close the message. You can verify the proNAS HA Event Log for further information.

Example of Replication status after selecting “**Yes**” to remove all replication:

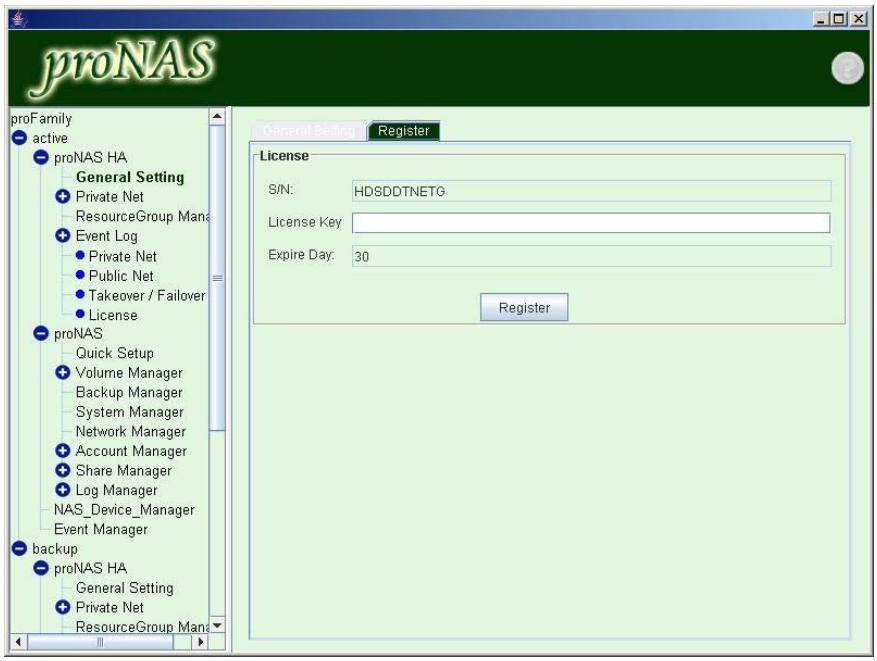


Example of Replication status after selecting "**No**" to retain all replication:

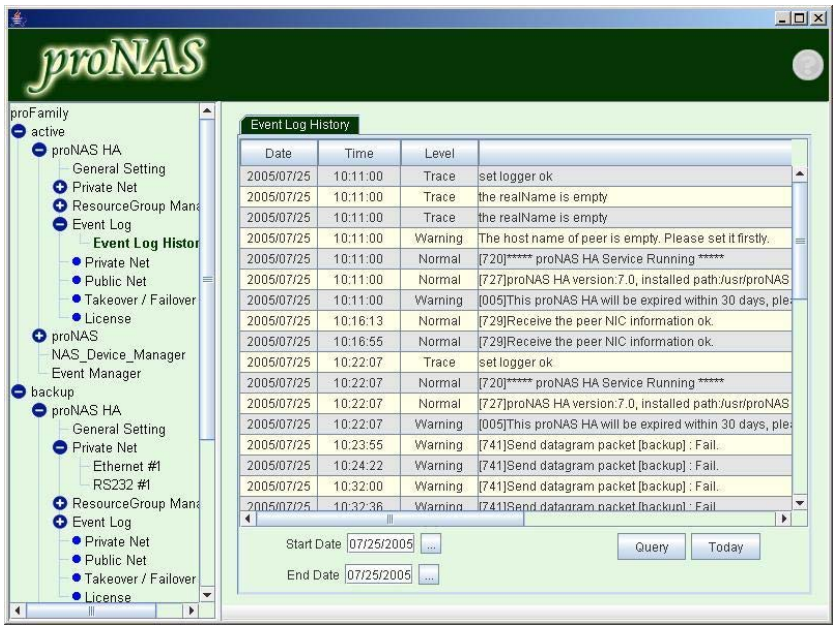


11.6 License Registration

To apply ProNAS HA license codes and register them to ProNAS HA users must first get the S/N of the two servers. Forward the S/N to your local ProNAS HA provider. Then Input the acquired License and click "Register" button. Users can now put ProNAS HA to work.



11.7 Event Log Properties


proNAS
proFamily
active
proNAS HA
General Setting
Private Net
ResourceGroup Mana
Event Log
Event Log Histor
Private Net
Public Net
Takeover / Failover
License
proNAS
NAS_Device_Manager
Event Manager
backup
proNAS HA
General Setting
Private Net
Ethernet #1
RS232 #1
ResourceGroup Mana
Event Log
Private Net
Public Net
Takeover / Failover
License
Event Log History
Date
Time
Level
2005/07/25 10:11:00 Trace set logger ok
2005/07/25 10:11:00 Trace the realName is empty
2005/07/25 10:11:00 Trace the realName is empty
2005/07/25 10:11:00 Warning The host name of peer is empty. Please set it firstly.
2005/07/25 10:11:00 Normal [720]***** proNAS HA Service Running *****
2005/07/25 10:11:00 Normal [727]proNAS HA version:7.0, installed path:/usr/proNAS
2005/07/25 10:11:00 Warning [005]This proNAS HA will be expired within 30 days, ple
2005/07/25 10:16:13 Normal [729]Receive the peer NIC information ok.
2005/07/25 10:16:55 Normal [729]Receive the peer NIC information ok.
2005/07/25 10:22:07 Trace set logger ok
2005/07/25 10:22:07 Normal [720]***** proNAS HA Service Running *****
2005/07/25 10:22:07 Normal [727]proNAS HA version:7.0, installed path:/usr/proNAS
2005/07/25 10:22:07 Warning [005]This proNAS HA will be expired within 30 days, ple
2005/07/25 10:23:55 Warning [741]Send datagram packet [backup] : Fail.
2005/07/25 10:24:22 Warning [741]Send datagram packet [backup] : Fail.
2005/07/25 10:32:00 Warning [741]Send datagram packet [backup] : Fail.
Start Date 07/25/2005
End Date 07/25/2005
Query
Today

All the messages generated by ProNAS HA will be displayed in the Event Log. The messages can help users to identify the possible reasons that prevent ProNAS HA from operating normally.